tellora

Administration

Base de données

PostgreSQL

Utilisateurs et privilèges

Rôles

- Postgres
  - Correspond au nom du compte utilisateur créé à l'installation de PostgreSQL
    - Il a tous les droits sur les objets (bases, tables, utilisateurs, …)
- Dans PostgreSQL un compte utilisateur est aussi appelé rôle
  - Un rôle est un objet global
    - C-à-d valable pour toute l'instance
  - Un rôle a des droits sur les objets, il peut ouvrir des connexions, il peut faire parti d'un autre rôle ou contenir d'autres rôles
    - Un rôle recouvre les notions d'utilisateurs et de groupes des versions précédentes à la version 8 de PostgreSQL

Rôles

- Créer un rôle
  - CREATE ROLE nomrole [[WITH] options […]]
    - Remplace les commandes CREATE USER et CREATE GROUPE des versions précédentes de PostgreSQL
    - Pour des raisons de compatibilité, ces commandes SQL existent toujours dans PostgreSQL
    - Commande également accessible à partir du système d'exploitation via la commande « createrole »
  - Exemple
    - CREATE ROLE charly LOGIN PASSWORD 'secret' CREATEDB ;
      - Création du compte CHARLY avec le mot de passe 'secret' et l'autorisation de se connecter à PostgreSQL et de créer des bases de données

Rôles

- Options de création d'un rôle

Option SQL	Option CLIENT	Description
LOGIN	-l	Indique si le rôle peut se connecter au serveur, le rôle devient l'équivalent d'un compte utilisateur
CONNECTION LIMIT limit_connexion	-c number	Indique le nombre maximum de connexions simultanées d'un rôle, valeur par défaut illimitée
[ENCRYPTED|UNENCRYPTED] PASSWORD 'mot de passe'	-P,-E,-N	Définit le mot de passe d'un rôle. ENCRYPTED et UNENCRYPTED indiques si le mot de passe doit être chiffré ou non
VALIDUNTIL 'date_heure'		Indique la date et l'heure de fin de validation du mot de passe. Par défaut le mot de passe est valable indéfiniment
SUPERUSER	-s	Indique que le rôle a tous les droits
CREATEDB	-d	Indique que le rôle peut créer des bases de données dans l'instance
CREATEROLE	-r	Autorise le rôle a créer d'autres rôles
IN ROLE nomrole [, …]		Indique le ou les rôles dont le rôle est membre
ROLE nomrole [,…]		Indique le ou les rôles qui deviennent membres du nouveau rôle, ce rôle devient un groupe
INHERIT	-i	Permet au rôle d'hériter des droits des rôles dont il est membre

Rôles

- Notion de groupe et d'héritage
  - La création d'un rôle sans le privilège LOGIN revient à la création d'un groupe
    - Un rôle qui a le privilège LOGIN peut aussi être un groupe
    - L'option «ROLE permet dés la création d'indiquer quels sont les rôles existants devenant membre de ce nouveau groupe
  - L'appartenance à un groupe ne fait pas hériter des privilèges du groupe
    - L'option INHERIT permet de rendre explicit cet héritage
  - Exemple
    - CREATE ROLE charly LOGIN PASSWORD 'secret' INHERIT IN ROLE groupe_admin ;
  - Lorsque l'héritage n'est pas défini à la création du rôle les privilèges du groupe ne sont pas transmis au rôle par défaut
    - La commande SET ROLE permet d'obtenir les privilèges du groupe
      - SET ROLE groupe_admin ;

Rôle

- Modification d'un rôle
  - S'effectue avec la commande
    - ALTER ROLE nomrole [[WITH] options […]] ;
  - Toutes les options de création d'un rôle sont utilisables (à condition d'avoir le droit de le faire)
    - Il suffit d'utiliser l'option pour ajouter le privilège
    - OU de préfixer par NO pour retirer l'option
  - Exemples
    - ALTER ROLE charly NOLOGIN ;
    - ALTER ROLE betty password 'nouveau_mot_passe' ;
    - ALTER ROLE betty RENAME TO minnie ;

Rôles

- Variables de sessions
  - L'ordre ALTER ROLE permet d'initialiser des variables de sessions propres au rôle afin que ces variables soient initialisées à l'ouverture de la session
    - La variable DateStyle permet de choisir le format affiché de la date
      - ALTER ROLE developpement SET datestyle='dmy' ;
    - La liste des variables est visualisable en utilisant la commande SHOW ALL dans PostgreSQL

Rôles

- Suppression d'un rôle
  - La suppression d'un rôle s'effectue avec l'ordre DROP ROLE nomrole
    - DROP ROLE developpement ;

Privilèges

- Le rôle créé, des privilèges peuvent leur être attribués en utilisant les commande
  - GRANT, attribue un privilège
  - REVOKE, retire un privilège
- Ces privilèges sont des privilèges objets correspondant à tous les objets existant dans le serveur PostgreSQL
  - Tables, database, function, langage, schema, tablespace

Privilèges

- Attribuer un privilège
  - GRANT privilèges [, privilèges2, …]
    ON type_objet nomobjet [, nomobjet2, ..]
    TO {nom_user [, nom_user2, …] | Public }
    [WITH GRANT OPTION] ;
    - Le mot clé PUBLIC correspond à tous les comptes utilisateurs, y compris ceux qui sont créés après l'attribution des droits
    - La clause WITH GRANT OPTION permet au rôle d'attribuer le privilège à un autre rôle
    - Exemple
      - Grant select, insert, update, delete
        on table clients, commande, ligue_comm TO charly ;

Privilèges

- Retirer un privilège
  - REVOKE privilèges [, privilèges2, …]
    ON type_objet nomobjet [, nomobjet2, ..]
    FROM {nom_user [, nom_user2, …] | Public }
    [CASCADE | RESTRICT] ;
    - Le mot clé PUBLIC correspond à tous les comptes utilisateurs, y compris ceux qui sont créés après l'attribution des droits
    - L'option CASCADE permet de retirer tous les droits sur un objet
    - Exemple
      - REVOKE select ON table clients from charly ;

Privilèges

- Liste des privilèges

Type objet	Privilège	Description
tous	ALL	Autorise tous les privilèges disponibles selon le type d'objet
table	SELECT	Droit de SELECT
	INSERT	Droit de INSERT
	UPRDATE	Droit de UPDATE
	DELETE	Droit de DELETE
	RULE	Droit de créer des rêgles sur la table
	TEMPORARY, TEMP	Droit de créer des tables temporaires
database	CREATE	Droit de créer une base de données
	REFERENCE	Droit de créer des clés étrangères depuis ou vers la table
function	EXECUTE	Droit d'exécuter une fonction
language	USAGE	Droit d'utiliser le langage procédurale
schema	CREATE	Droit de créer des tables dans le schéma
	USAGE	Droit d'utiliser les objets contenus dans le schéma
tablespace	create	Droit de créer des tables et des index dans le tablespace

Privilèges

- Gestion de l'appartenance à un rôle
  - Les commandes GRANT et REVOKE permettent d'ajouter ou de supprimer un rôle comme membre d'un autre rôle
    - GRANT role [, ..] TO nomrole [, ..] [WITH ADMIN OPTION] ;
    - REVOKE [ADMIN OPTION FOR] role [, …] FROM nomrole [, …] [CASCADE|RESTRICT] ;
    - EXEMPLE
      - GRANT ROLE developpement TO exploitation ;

Travaux pratiques

- Dans le cahier de travaux pratiques
  - Faire l'exercice 04_créer users
  - Pour cela utiliser le répertoire :
    - TP_Postgres\04_creeusers