Habilitations en bases de données

Pour préserver la confidentialité des données au sein d'un SGBD, il est nécessaire d'établir une politique de droits d'accès. Cette politique sera fondée sur les éléments suivants :

- des objets (tables, vues, etc.) ;
- des utilisateurs ;
- des droits ;
- et, pour faciliter la gestion, des groupes d'utilisateurs.

Une politique de droits définira aussi précisément que possible “**qui a quels droits sur quels objets ?**”.

Gestion des utilisateurs

La gestion des utilisateurs suppose la possibilité de créer, modifier ou supprimer un utilisateur.

Créer un utilisateur

Ci-contre, une version simple de création d'un utilisateur	`CREATE USER nomUtilisateur IDENTIFIED BY 'motDePasse';`

Modifier un utilisateur

Ci-contre, une version simple de modification d'un utilisateur	`ALTER USER nomUtilisateur IDENTIFIED BY 'nouveau_mdp';`

Supprimer un utilisateur

Ici, la suppression d'un utilisateur	`DROP USER nomUtilisateur;`

Gestion des droits

La gestion des droits suppose la possibilité d'attribuer ou de retirer des droits.

Attribution de droits

Là, une attribution de droit	`GRANT droit1 [, droit2 [, ...]]`
	`ON nomObjet`
	`TO nomUtilisateur;`

Retrait de droits

Et ici, un retrait de droit	`REVOKE droit1 [, droit2 [, ...]]`
	`ON nomObjet`
	`FROM nomUtilisateur;`

Gestion des groupes d'utilisateurs

Les groupes d'utilisateurs, nommés “**Rôles**” dans l'univers SQL, permettent de rendre plus aisée la gestion des droits lorsque le nombre d'utilisateurs grandit et que les droits de chacun correspondent à des modèles, tels des profils d'utilisateurs.

Création des groupes (rôles)

Ci-contre, une version simple de création de groupe	`CREATE ROLE nomRôle;`

Affectation des utilisateurs au groupe

Ci-contre, une version simple d'affectation des utilisateurs aux groupes	`GRANT nomRôle TO nomUtilisateur;`

Affectation des droits au groupe

Ci-contre, une version simple d'affectation des droits aux groupes	`GRANT {priv1[,priv2,...]|ALL}`
	`ON objet`
	`TO nomRôle;`

Activation des groupes

La problématique des droits sur des sous-ensembles de données

il s'agit de permettre à certains utilisateurs d'accéder uniquement à une partie spécifique des données (certaines lignes, certaines colonnes) plutôt qu'à l'ensemble de la table ou de la base. Cette approche est essentielle pour respecter les principes du besoin d'en connaître, de la confidentialité des données et des exigences réglementaires comme le RGPD

Création d'une vue qui présente les données souhaitées

Ci-contre, une version simple de création de vue:	`CREATE VIEW nomVue AS`
	`SELECT colonne1, colonne2...`
	`FROM TABLE`
	`WHERE condition;`

Attribution des droits à la vue

Ci-contre, une version simple d'attribution des droits à la vue:	`GRANT {SELECT, INSERT, UPDATE, DELETE}`
	`ON nomVue`
	`TO nomRôle;`

From:
https://wiki.siochaptalqper.fr/ - **Wiki SIO Chaptal**

Permanent link:
https://wiki.siochaptalqper.fr/doku.php?id=bloc3:habilitationsbd

Last update: **2025/04/30 14:06**