

Programmation Web Dynamique II

15. Gestion des droits et des usagers

Utilisateurs et privilèges

- Tout système de gestion de base de données implémente le système d'utilisateurs et de privilèges.
 - Chaque utilisateur du système possède un nom d'utilisateur et un mot de passe permettant de s'authentifier avec le système.
 - À chaque utilisateur est relié un ensemble de privilèges (sélection, création, modification, suppression) qui peut être attribué sur :
 - Chacune des bases
 - Chacune des tables
 - Chacune des colonnes
 - Chacune des fonctions stockées dans la BD (dépassé le cadre du cours)
- En MySQL, les usagers ainsi que leurs droits (ou privilèges) sont stockés dans une base de données nommée `mysql` sur le serveur.
- Il est donc possible de modifier directement les usagers et leurs privilèges dans la BD en accédant aux tables de cette base de données.
- Toutefois, il est généralement plus pratique de le faire à partir des instructions MySQL qui manipulent indirectement ces tables.

Création d'utilisateurs

- On peut créer de nouveaux utilisateurs dans le système en utilisant l'instruction suivante :
 - `CREATE USER 'login'@'hôte' IDENTIFIED BY 'mot_de_passe'`, où le mot de passe est optionnel.
 - Ex : `CREATE USER 'gharvey'@'195.5.33.22' IDENTIFIED BY '12345'`
 - Ex : `CREATE USER 'testSansPassword'@'localhost'`
- Le premier élément à spécifier est le login, qui sera le nom d'utilisateur que cet utilisateur devra utiliser.
- Le second élément est l'hôte, qui détermine à partir de quelle adresse se connectera l'utilisateur. Dans notre cas, ce sera généralement localhost puisque notre utilisateur servira dans des scripts PHP qui sont sur le même serveur que la base de données. L'hôte est facultatif : si vous n'en spécifiez pas, l'utilisateur pourra utiliser ce nom d'utilisateur à partir de n'importe quelle adresse pour se connecter.
- Le mot de passe spécifie le mot de passe que l'utilisateur doit utiliser pour se connecter.

Modification et suppression des usagers

- On peut modifier un nom d'utilisateur avec l'instruction rename selon la syntaxe suivante :
 - `RENAME USER ancien TO nouveau`
 - Ex : `RENAME 'gharvey'@'localhost' TO 'guillaumeh'@'localhost'`
- On peut modifier le mot de passe d'un utilisateur avec l'instruction ALTER USER
 - Ex : `ALTER USER 'gharvey'@'localhost' IDENTIFIED BY '12345'`
- La **suppression** d'un utilisateur se fait avec l'instruction DROP USER.
 - Ex : `DROP USER 'gharvey'@'localhost'`

Privilèges

- Un usager nouvellement créé n'a aucun privilèges et ne peut donc que se connecter. Il faut attribuer les privilèges après la création de l'utilisateur.
- Pour donner un privilège, il faut évidemment que l'utilisateur courant ait le privilège de pouvoir donner un privilège!
 - Ce privilège s'appelle GRANT OPTION.
- L'instruction pour donner un privilège va comme suit :
 - GRANT nomDuPrivilège [listeColonnes] ON niveauDuPrivilège TO 'nomUsager'@'hote', où :
 - La liste de colonnes est facultative
 - Il est possible de spécifier plusieurs noms de privilèges couplés à des listes de colonnes dans la même requête.
 - Il est possible d'utiliser *.* pour toutes les bases de données et toutes les tables, ou encore ligue.* pour toutes les tables dans la base de données ligue.
 - Ex : GRANT SELECT ON ligue.joueur TO 'gharvey'@'localhost'
 - Ex : GRANT SELECT, UPDATE(prenom, nom), INSERT ON ligue.joueur TO 'gharvey'@'localhost'
- Les noms de privilèges que l'on peut accorder sont :
 - SELECT, INSERT, UPDATE, DELETE pour les requêtes de type CRUD.
 - CREATE TABLE, DROP pour les requêtes sur les tables
 - ALL, qui contient tous les privilèges
 - GRANT OPTION, qui permet de créer des usagers et d'assigner des privilèges.
 - Il y a aussi d'autres privilèges spécifiques pour les fonctions stockées et les vues, ce qui dépasse le