Utilisateurs et privilèges

Introduction

Tout le monde a-t-il le droit de voir, insérer, modifier et effacer toutes les données ?

- ⇨ Mise en place de permission bien spécifique pour chaque utilisateur
- ⇨ Un utilisateur est identifié par un login mais également par la machine à partir de laquelle il se connecte à la DB (hostname ou IP – voir cours réseau)

Stockage des infos (User et permission) dans la DB système « MYSQL »

- ⇨ Liste des utilisateurs : SELECT user, host FROM user;

- ⇨ Qui est logué : SELECT user() ;

- ⇨ 2 actions :
  - Créer un utilisateur
  - Lui donner les droits adéquats

Création User

Création :

CREATE USER 'pol'@'localhost' IDENTIFIED BY 'pol';

Remarques :

- Password et Domaine sont facultatif :
  - CREATE USER luc;
- Le domaine :
  - « localhost »
  - « 192.168.23.48 »
  - « 10.235.14.% »
  - « le_nom_du_domaine »
  - « % »

Changement de password :

SET PASSWORD FOR 'pol'@'localhost' = PASSWORD('polo');

Changement de Domaine :

UPDATE mysql.user SET Host='10.12.45.%' WHERE Host='localhost' AND User='pol';

Suppression :

DROP USER 'pol'@'localhost';

Ejection d'un user (par un DBA !) :

SHOW Processlist;
KILL 6;

Privilèges d'un User

Liste des Privilèges (droits) :

SHOW GRANTS FOR 'pol'@'localhost';

Remarque :

- GRANT USAGE ON *.* TO 'pol'@'localhost' => AUCUN privilège

Qui donne ?

ROOT ou un user avec « WITH GRANT OPTION » (voir Ult)

Privilèges :

Autorisation d'effectuer une action sur un objet de la DB

- Notation : DB.Table.Colonne (ex : ecole.t_pers.nom)

Accès à TOUT **SANS** pouvoir donner les privilèges à d'autres

- GRANT ALL PRIVILEGES ON *.* TO 'pol'@'localhost'; (toutes les DB)
- GRANT ALL PRIVILEGES ON ecole.* TO 'pol'@'%'; (toutes les Tables)

Pour que l'utilisateur puisse octroyer des privilèges à d'autre

- GRANT ALL PRIVILEGES ON ecole.* TO 'pol'@'%' WITH GRANT OPTION;
- GRANT SELECT, UPDATE, GRANT OPTION ON … (autre syntaxe)

Mise à jour de la DB système pour que les droits soient actifs

- FLUSH PRIVILEGES ;

Droits spécifiques de base

- Action : CREATE, ALTER, DROP, SELECT, UPDATE, INSERT, DELETE
- Objet : *.*, ecole.*, tintin.album, ecole. Tropcoursetud, *, …

- Exemples :

```
GRANT SELECT(nom, prenom), UPDATE(prenom)
ON ecole.T_Pers TO 'pol'@'localhost';

GRANT CREATE, DROP
ON TABLE tintin.* TO zoe@localhost;
```

Droits spécifiques sur les Procédures stockées

- Action : CREATE ROUTINE, EXECUTE
- Objet : *.*, ecole.*, tintin.album, ecole. Tropcoursetud, *, …

- Exemples :

```
GRANT CREATE ROUTINE, EXECUTE
ON tintin.*
TO 'pol'@'localhost';
```

Remarques :

- Les vues sont considérées comme de vulgaires tables
- Pour une vue, procédure, trigger, … => les privilèges du créateur seront pris en compte (SELECT pas obligatoire le cas échéant) mais il faut le privilège EXECUTE !

Suppression de privilège :

Partiel

- REVOKE DELETE ON tintin.album FROM 'leon'@'10.2.25.147';

Global (Supprime TOUS les droits sur le serveur)

- REVOKE ALL PRIVILEGES, GRANT OPTION FROM 'pol'@'localhost';

A TESTER :

- Est-il possible de supprimer un utilisateur s'il a toujours des privilèges ?
- Quels sont les privilèges accordés lors de la création d'un user ?
- Qui peut créer un user et à quelle condition ?
- Qui peut donner des privilèges à un user et à quelle condition ?
- Peut-on voir les droits des autres users ?

Exercices :

1. Créer 2 users : Marcel et Lucien

2. Donner les privilèges à Marcel sur ecole.t_Pers avec possibilité d'en donner

3. Ouvrir les sessions : Marcel et Lucien

4. Contrôler pour les 2 sessions :
   SELECT * FROM T_Pers WHERE PK_Pers < 10;
   SELECT * FROM T_Prof WHERE PK_Pers < 10;

5. Marcel peut-il donner des privilèges à Lucien sur T_Prof ?

6. Marcel donne les privilèges sur T_Pers à Lucien :

7. Marcel retire les privilèges sur T_Pers à Lucien :
   REVOKE ALL PRIVILEGES ON ecole.t_pers FROM luc@localhost ;