Système d'information et base de données

CM3 : Droits des utilisateurs MySQL

Mickaël Martin Nevot

V2.2.1

Système d'information et base de données

Sécurité des accès

« priv » = privilèges

- **Base de données d'administration** propre (par défaut `/var/lib/mysql/mysql`) pour gérer la sécurité des accès aux autres bases de données
- Seul l'utilisateur `root` de MySQL devrait y avoir accès
- La base de données `mysql` utilise cinq tables pour décider « qui » a la permission de faire « quoi » sur quelle « base de données », à partir « de quelle machine » :
  - `user` : informations générales de sécurité
  - `host` : machines ayant le droit d'accéder au serveur
  - `db`, `tables_priv`, `columns_priv` : droits d'accès pour une base de données, une table ou une colonne

Tables de droits

Nom de la table	user	db	host
Identifiant	Host	Host	Host
	User	Db	Db
	Password	User	
Champs de droits	Select_priv	Select_priv	Select_priv
	Insert_priv	Insert_priv	Insert_priv
	Update_priv	Update_priv	Update_priv
	Delete_priv	Delete_priv	Delete_priv
	Index_priv	Index_priv	Index_priv

priv = privilèges

Dans les tables user, db et host, tous les champs de droits sont déclarés avec le type ENUM('N','Y') : ils peuvent prendre les valeurs N (non) ou Y (oui) et la valeur par défaut est N

Tables de droits

Nom de la table	user	db	host
Champs de droits	Alter_priv	Alter_priv	Alter_priv
	Create_priv	Create_priv	Create_priv
	Drop_priv	Drop_priv	Drop_priv
	Grant_priv	Grant_priv	Grant_priv
	References_priv	…	…
	Reload_priv		
	Shutdown_priv		
	Process_priv		
	File_priv		
	…		

Tables de droits

Nom de la table	tables_priv	columns_priv
Identifiant	Host	Host
	Db	Db
	User	User
	Table_name	Table_name
		Column_name
Champs de droits	Table_priv	Column_priv
	Column_priv	
Autre champs	Timestamp	Timestamp
	Grantor	

Types des champs d'identification

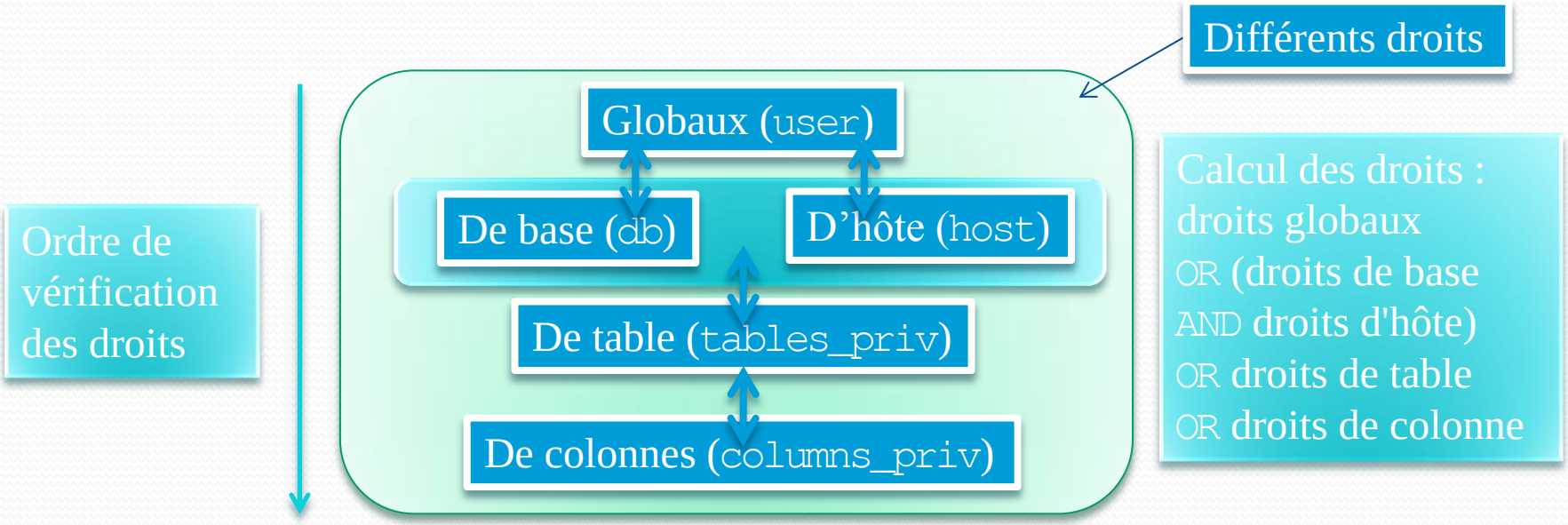
Nom du champs	Type	Notes
Host	CHAR(60)	
User	CHAR(16)	
Password	CHAR(41)	
Db	CHAR(64)	CHAR(60) pour les tables tables_priv et columns_priv
Table_name	CHAR(60)	
Column_name	CHAR(60)	

Champs encrypté de 40 caractères et commençant toujours par *. Longtemps ce champs a été de type CHAR(16), pouvant créer des problèmes de compatibilité

Les valeurs des colonnes User, Password , Db et Table_name sont sensibles à la casse ; celles de Host et Column_name sont insensibles à la casse (depuis MySQL 3.22.12)

Contrôle d'accès

- Le serveur vérifie l'autorisation de connexion
- Le serveur vérifie chaque requête pour vérifier si les droits sont suffisants pour l'exécuter



Pas de groupes ou de rôles en MySQL, ce n'est même pas prévu pour la version 6

Permissions MySQL

Commande MySQL : `show privileges`

- Privilèges globaux (non spécifiques à une base de données) :
  - `RELOAD` : droit de relance du serveur `mysqld` et d'écriture des tables « sur disque »
  - `SHUTDOWN` : droit d'arrêter le serveur `mysqld`
  - `PROCESS` : droit de contrôler les processus utilisateurs
  - `FILE` : droit d'écrire ou lire dans des fichiers avec les commandes `LOAD DATA` et `INTO OUTFILE`
- Privilèges spécifiques :
  - `SELECT` : droit d'effectuer des recherches
  - `INSERT` : droit d'effectuer des insertions
  - `UPDATE` : droit d'effectuer des mises à jour
  - `DELETE` : droit d'effectuer des destructions d'enregistrements

Permissions MySQL

- Privilèges spécifiques :
  - `INDEX` : droit de créer ou détruire des index de tables
  - `ALTER` : droit de modifier la structure des tables
  - `CREATE` : droit de créer des bases de données ou des tables
  - `USAGE` : droit de se connecter au serveur (uniquement)

    Utile uniquement pour changer le mot de passe de connexion
  - `LOCK` : droit de verrouiller/déverrouiller des tables
  - `DROP` : droit de détruire des bases de données ou des tables
  - `GRANT` : droit d'affecter ou retirer des droits à un utilisateur
  - `REFERENCES` : droit lié aux clefs étrangères (obsolète)

Allouer les permissions

- **GRANT :** permet de **créer un utilisateur**, lui allouer des **droits** et changer son **mot de passe** :

```
mysql> GRANT ALL ON test.* TO user IDENTIFIED BY 'pwd';
mysql> GRANT SELECT, INSERT ON mysql.* TO user@localhost IDENTIFIED BY 'pwd';
mysql> GRANT SELECT, INSERT ON mysql.* TO user@localhost IDENTIFIED BY 'pwd' WITH GRANT
OPTION;
mysql> GRANT FILE ON *.* TO user@localhost;
```

Syntaxe :

```
GRANT priv_type [(column_list)] [, priv_type [(column_list)]]
ON {tbl_name | * | *.* | db_name.*}
TO user [IDENTIFIED BY [PASSWORD] 'password']
```

Commande MySQL : `SHOW GRANTS FOR user@localhost`

Allouer les permissions

- Permissions :

Les privilèges SELECT, INSERT sont placés dans la table db pour une base de données

```
mysql> SELECT * FROM db WHERE user= 'user';
Host Db User Select_priv Insert_priv Update_priv Delete_priv Create_priv Drop_priv
Grant_priv References_priv Index_priv Alter_priv
| localhost | mysql | user | Y | Y | N | N | N | N | N | N| N | N | N | N |

mysql> SELECT * FROM user WHERE user= 'user';
Host User Password Select_priv Insert_priv Update_priv Delete_priv Create_priv Drop_priv
Reload_priv Shutdown_priv Process_priv File_priv Grant_priv References_priv Index_
| localhost | user | 398e7500242ab90c | N | N | N | N | N | N | N| N | N | N | N | N | N
| N | N | N | N| N | N | N | N | |
```

- Changer de mot de passe :

```
mysql> GRANT USAGE ON *.* TO user@localhost IDENTIFIED BY 'pwd';
```

Commande de diagnostic utile : mysqlaccess

Supprimer des permissions

- Ôter des permissions (REVOKE) :

```
mysql> REVOKE ALL ON *.* FROM user;
mysql> REVOKE ALTER, DELETE, DROP ON mysql.* FROM user;
mysql> REVOKE GRANT OPTION ON mysql.* FROM user@localhost;
mysql> REVOKE SELECT on mysql.* FROM user@localhost;
```

Syntaxe :

```
REVOKE priv_type [(column_list)] [, priv_type [(column_list)]]
ON {tbl_name | * | *.* | db_name.*} FROM user [, user]
```

- Supprimer un utilisateur :
  - A partir de la version 4.1.1 :

```
mysql> REVOKE ALL PRIVILEGES FROM user@localhost;
mysql> DROP USER user;
```

  - Versions antérieures :

```
mysql> DELETE FROM mysql.user WHERE User='user' AND Host='host';
```

  - Recharger les permissions en mémoire :

```
mysql> FLUSH PRIVILEGES;
```

Liens

- Documents électroniques :
  - http://www.elliptic.fr/doc/mysql
  - http://dev.mysql.com/doc/refman/5.5/en
- Documents classiques :
  - Cours :
    - Maurice Libes. *Administration et exploitation du SGBDR MySQL*.
    - Cyril Gruau. *Conception d'une base de données*.
    - Jean-Marc Petit. *Administration des bases de données*.

Crédits

Auteur

Mickaël Martin Nevot
mmartin.nevot@gmail.com

Carte de visite électronique

Relecteurs

Cours en ligne sur : www.mickael-martin-nevot.com