

# Langage de contrôle des données (DCL): Gestion des utilisateurs

Dr. Mamadou Camara<sup>(1)</sup>

<sup>(1)</sup>ESP, Cheikh Anta Diop University, Dakar, Senegal  
mamadou.camara@ucad.edu.sn

Module OMGL3

## Fonctionnalités d'un SGBD relatives au DCL

pour protéger les données l'utilisation non autorisée délibérée ou accidentelle :

- ▶ Les utilisateurs doivent être connus de Mysql avant qu'ils ne puissent accéder aux données de la base.
- ▶ Un mot de passe peut être assigné à chaque utilisateur SQL.
- ▶ Les privilèges peuvent être accordés aux utilisateurs.

## Les niveaux de privilèges

les différents niveaux de privilèges que l'on peut rencontrer

1. Privilèges utilisateur sont liés à toutes les bases de données qui sont connues de mysql, par exemple le privilège de supprimer une base existante ou d'en créer une nouvelle.
2. Les privilèges de base de données sont liés à toutes les tables d'une base de données spécifique, par exemple le privilège de créer de nouvelles tables dans une base de données IUT existante.

## Les niveaux de privilèges

les différents niveaux de privilèges que l'on peut rencontrer

1. Les privilèges de table sont liés à toutes les données d'une table spécifique, par exemple le privilège de consulter toutes les données de la table enseignant avec des clauses Select.
2. Les privilèges de colonne sont liés à une colonne spécifique d'une table, tel que le privilège de mettre à jour les valeurs de la colonne note de la table notes avec des commandes Update.
3. Les privilèges routine sont assignés au niveau des sous-programmes catalogués (fonction ou procédure)

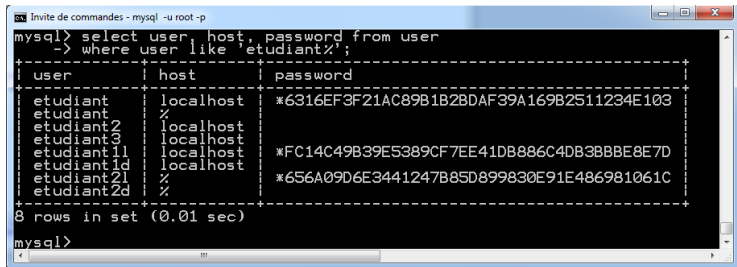
## Ajout

- ▶ Pour ajouter un utilisateur dans le catalogue, Mysql utiliser la commande CREATE USER
- ▶ Dans une commande CREATE USER, un nom d'utilisateur et un password sont entrés.
- ▶ Ne pas spécifier d'hôte équivaut à spécifier "%" comme hôte.
- ▶ Si aucun password n'est entré, l'utilisateur concerné est autorisé à se connecter sans password.

## Ajout

```
1 create user 'etudiant1l'@'localhost'  
2 identified by 'etudiant';  
3  
4 create user 'etudiant1d'@'localhost' ;  
5  
6 create user 'etudiant2l'@'%'  
7 identified by 'etudiant2';  
8  
9 create user 'etudiant2d' ;  
10  
11 select user, host, password from user  
12 where user like 'etudiant%';
```

## Ajout



Invite de commandes - mysql -u root -p

```
mysql> select user, host, password from user  
-> where user like 'etudiant%';
```

user	host	password
etudiant	localhost	*6316EF3F21AC89B1B2BDAF39A169B2511234E103
etudiant	%	
etudiant2	localhost	
etudiant3	localhost	
etudiant11	localhost	*FC14C49B39E5389CF7EE41DB886C4DB3BBBE8E7D
etudiant1d	localhost	
etudiant21	%	*656A09D6E3441247B85D899830E91E486981061C
etudiant2d	%	

8 rows in set (0.01 sec)

```
mysql>
```

## Ajouts multiples et renommer utilisateur

- Possible de créer plusieurs utilisateurs en une commande

```
1 CREATE USER
2 'CHRISTIAN'@'localhost' IDENTIFIED BY 'CHRISTIANPASSER',
3 'PAUL'@'localhost' IDENTIFIED BY 'PAULPASSER';
```

```
35 rename user 'etudiant2'@'localhost'
36 to 'etudiant4'@'localhost';
37
```



## MAJ password

Un utilisateur a la possibilité de changer son password ou celui d'un autre, en utilisant

- ▶ la commande SET PASSWORD.
- ▶ ou la commande update

La fonction password permet d'encriper le mot de passe

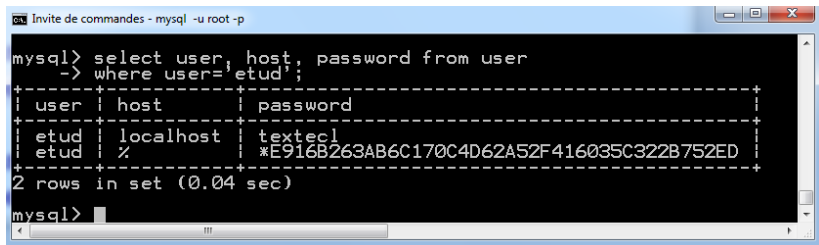
- ▶ SET PASSWORD exige un mot de passe au format encrpté
- ▶ CREATE USER encrpte automatiquement

## MAJ password

```
38 set password for
39 'etudiant'@'localhost' = password('newpssw');
```

```
16 update user set password='textec1' where
17 user = 'etud';
18
19 update user set password=PASSWORD('textec1')
20 where user = 'etud' and host='%';
21
22 select user, host, password from user
23 where user='etud';
```

## MAJ password



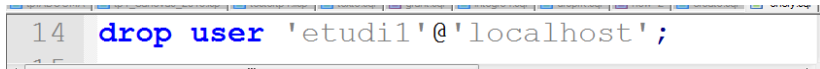
The screenshot shows a terminal window titled "Invite de commandes - mysql -u root -p". The user has entered the command `mysql> select user, host, password from user -> where user='etud';`. The output is a table with two rows. The first row shows user 'etud' on localhost with password 'textec1'. The second row shows user 'etud' on '%' with password '\*E916B263AB6C170C4D62A52F416035C322B752ED'. Below the table, it says "2 rows in set (0.04 sec)". The prompt `mysql>` is visible at the bottom.

```
mysql> select user, host, password from user
-> where user='etud';
+-----+-----+-----+
| user | host   | password |
+-----+-----+-----+
| etud | localhost | textec1 |
| etud | %       | *E916B263AB6C170C4D62A52F416035C322B752ED |
+-----+-----+-----+
2 rows in set (0.04 sec)

mysql>
```

## Suppression

- ▶ La commande DROP USER est utilisée,
- ▶ Elle supprime automatiquement, tous les privilèges de l'utilisateur.
- ▶ Si l'utilisateur avait créé des tables, des indexes, ou d'autres objets de bases de données, ces objets ne sont pas supprimés car Mysql n'enregistre pas qui a créé les objets.



```
14 drop user 'etudi1'@'localhost';
```

- └ Accorder des privilèges
  - └ Accorder des privilèges de table et de colonne

## Privilèges de table et de colonne

- ▶ Si les privilèges sont accordés à un utilisateur qui n'existe pas encore, MySQL crée cet utilisateur en exécutant automatiquement la commande CREATE USER.

```
1 GRANT SELECT
2 ON ENSEIGNANT
3 TO 'BAH'@'localhost' IDENTIFIED BY 'BAHPASS'
4
5 GRANT INSERT, UPDATE
6 ON ENSEIGNANT
7 TO BAH, PAUL
8
9 GRANT UPDATE (IDMAT, RESPONSABLE)
10 ON MATIERE
11 TO PAUL
```

- └ Accorder des privilèges
- └ Accorder des privilèges de table et de colonne

## Columns\_priv

```
Invite de commandes - mysql -u root -p
25 rows in set (0.11 sec)
mysql> describe columns_priv;
+-----+-----+-----+-----+
| Field | Type | Null | Key |
+-----+-----+-----+-----+
| Host  | char(60) | NO | PRI |
| Db    | char(64) | NO | PRI |
| User  | char(16) | NO | PRI |
| Table_name | char(64) | NO | PRI |
| Column_name | char(64) | NO | PRI |
| Timestamp | timestamp | NO | PRI |
| Column_priv | set('Select','Insert','Update','References') | NO | PRI |
+-----+-----+-----+-----+
7 rows in set (0.00 sec)

mysql> █
```

- tables\_priv contient une colonne column\_priv qui fait la synthèse de droits attribués au niveau colonne pour chaque table

- └─ Accorder des privilèges
- └─ Accorder des privilèges de table et de colonne

## Tables\_priv1

```
mysql -u root -p
7 rows in set (0.00 sec)
mysql> describe tables_priv;
+-----+-----+-----+-----+-----+
| Field | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+
| Host | NO | PRI | char(60) | |
| Db | NO | PRI | char(64) | |
| User | NO | PRI | char(16) | |
| Table_name | NO | PRI | char(64) | |
| Grantor | NO | MUL | char(77) | |
| Timestamp | NO | | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
| Table_priv | NO | | set('Select','Insert','Update','Delete','Create','Drop') | |
| Column_priv | NO | | set('Select','Insert','Update','References') | |
+-----+-----+-----+-----+-----+
8 rows in set (0.00 sec)
```

- └ Accorder des privilèges
- └ Accorder des privilèges de table et de colonne

## Tables\_priv2

```
Invite de commandes - mysql -u root -p
-----
-+
|
|-----
-+
|
|
|
|
|
|
|
|
|
|
op', 'Grant', 'References', 'Index', 'Alter', 'Create View', 'Show view', 'Trig
|
|-----
-+
```

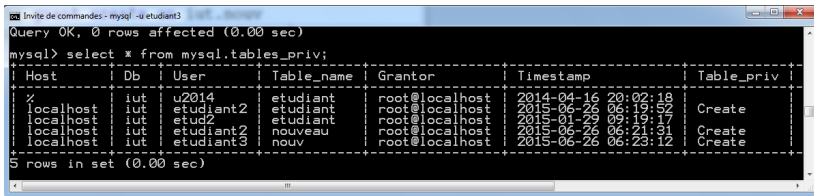


- └ Accorder des privilèges
  - └ Accorder des privilèges de table et de colonne

## Tables\_priv3 : create

- Le privilège create est accordé à Etudiant3 en local sur une table nommée "nouv" de la base iut.

```
13 grant create on iut.nouv
14 to 'etudiant3'@'localhost';
```



Invite de commandes - mysql -u etudiant3

Query OK, 0 rows affected (0.00 sec)

mysql> select \* from mysql.tables\_priv;

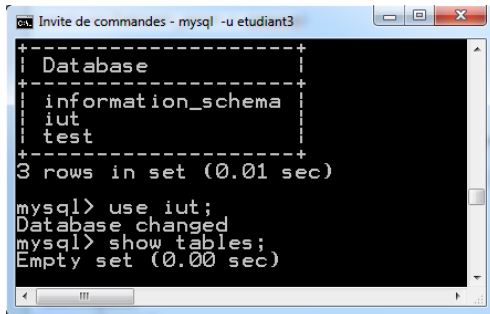
Host	Db	User	Table_name	Grantor	Timestamp	Table_priv
%	iut	u2014	etudiant	root@localhost	2014-04-16 20:02:18	
localhost	iut	etudiant2	etudiant	root@localhost	2015-06-26 06:19:52	Create
localhost	iut	etud2	etudiant	root@localhost	2015-06-26 06:19:52	
localhost	iut	etudiant2	nouveau	root@localhost	2015-06-26 06:21:31	Create
localhost	iut	etudiant3	nouv	root@localhost	2015-06-26 06:23:12	Create

5 rows in set (0.00 sec)

- └ Accorder des privilèges
  - └ Accorder des privilèges de table et de colonne

## Tables\_priv4 : create

- ▶ Etudiant3 n'a pas accès aux autres bases différentes
  - ▶ show databases donne iut.
- ▶ Il n'a pas accès aux tables déjà créées dans la base iut ;
  - ▶ show tables donne l'ensemble vide



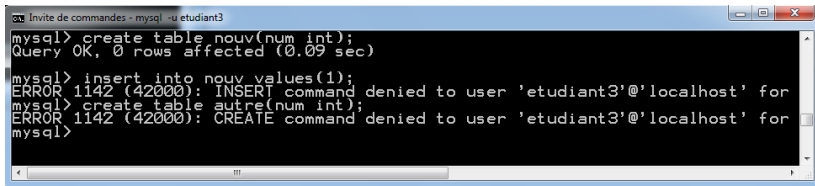
```
Invite de commandes - mysql -u etudiant3
+-----+
| Database |
+-----+
| information_schema |
| iut |
| test |
+-----+
3 rows in set (0.01 sec)

mysql> use iut;
Database changed
mysql> show tables;
Empty set (0.00 sec)
```

- └ Accorder des privilèges
  - └ Accorder des privilèges de table et de colonne

## Tables\_priv5 : create

- ▶ Il a le droit de créer une table nommée "nouv"
- ▶ Le droit de créer est différent de celui d'insérer.



```
mysql> create table nouv(num int);
Query OK, 0 rows affected (0.09 sec)

mysql> insert into nouv values(1);
ERROR 1142 (42000): INSERT command denied to user 'etudiant3'@'localhost' for
mysql> create table autre(num int);
ERROR 1142 (42000): CREATE command denied to user 'etudiant3'@'localhost' for
mysql>
```

## Privilèges de base de données

- ▶ Les privilèges de table s'appliquent à une table spécifique.
- ▶ Mysql supporte aussi des privilèges pour une base de données dans son ensemble, par exemple le privilège de créer des tables ou des vues dans une base spécifique.
- ▶ \* représente la base en cours (e.i. celle sélectionné avec use)

- └ Accorder des privilèges
- └ Accorder des privilèges de base de données

## Privilèges de base de données : Exemple

```
1 GRANT SELECT
2 ON IUT.*
3 TO BAH
4
5 GRANT CREATE, ALTER, DROP, CREATE VIEW
6 ON IUT.*
7 TO PAUL
8
9 GRANT SELECT
10 ON INFORMATION_SCHEMA.*
11 TO PAUL
12 # SELECT, INSERT dans toutes les tables de la base
13 GRANT SELECT, INSERT
14 ON *
15 TO CHRISTIAN
```

- └─ Accorder des privilèges
- └─ Accorder des privilèges de base de données

## Privilèges de base de données

```
Invite de commandes - mysql -u root -p
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> use mysql;
Database changed
mysql> desc db;
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| Host | char(60) | NO | PRI | | |
| Db | char(64) | NO | PRI | | |
| User | char(16) | NO | PRI | | |
| Select_priv | enum('N','Y') | NO | | N | |
| Insert_priv | enum('N','Y') | NO | | N | |
| Update_priv | enum('N','Y') | NO | | N | |
| Delete_priv | enum('N','Y') | NO | | N | |
| Create_priv | enum('N','Y') | NO | | N | |
| Drop_priv | enum('N','Y') | NO | | N | |
| Grant_priv | enum('N','Y') | NO | | N | |
| References_priv | enum('N','Y') | NO | | N | |
| Index_priv | enum('N','Y') | NO | | N | |
| Alter_priv | enum('N','Y') | NO | | N | |
| Create_tmp_table_priv | enum('N','Y') | NO | | N | |
| Lock_tables_priv | enum('N','Y') | NO | | N | |
| Create_view_priv | enum('N','Y') | NO | | N | |
| Show_view_priv | enum('N','Y') | NO | | N | |
| Create_routine_priv | enum('N','Y') | NO | | N | |
| Alter_routine_priv | enum('N','Y') | NO | | N | |
| Execute_priv | enum('N','Y') | NO | | N | |
| Event_priv | enum('N','Y') | NO | | N | |
| Trigger_priv | enum('N','Y') | NO | | N | |
+-----+-----+-----+-----+-----+-----+
22 rows in set (0.01 sec)
```

## Accorder des privilèges utilisateur

- ▶ Les privilèges qui ont la portée la plus large sont les privilèges utilisateur.
- ▶ Pour toutes les commandes pour lesquels des privilèges de base de données peuvent être attribués, les privilèges utilisateur peuvent être attribués aussi.
- ▶ Par exemple, en accordant à quelqu'un un privilège CREATE au niveau utilisateur, cet utilisateur peut créer de nouvelles bases de données mais aussi des tables dans toutes les bases de données.

## Accorder des privilèges utilisateur

Mysql supporte aussi les privilèges utilisateur, par exemple :

- ▶ créer ou supprimer des utilisateurs.
- ▶ consulter la liste de toutes les bases de données avec la commande `SHOW DATABASES`.



## Accorder des privilèges utilisateur

Dans l'exemple suivant

- ▶ CHRISTIAN a les privilèges de création, de suppression et de modifications sur toutes les bases de données existantes et futures.
- ▶ PAUL peut créer de nouveaux utilisateurs.

- └ Accorder des privilèges
  - └ Accorder des privilèges utilisateur

## Accorder des privilèges utilisateur

```
1 GRANT CREATE, ALTER, DROP
2 ON *.*
3 TO CHRISTIAN
4
5 GRANT CREATE USER
6 ON *.*
7 TO PAUL
8
9 GRANT ALL PRIVILEGES
10 ON *.*
11 TO ROOT
```

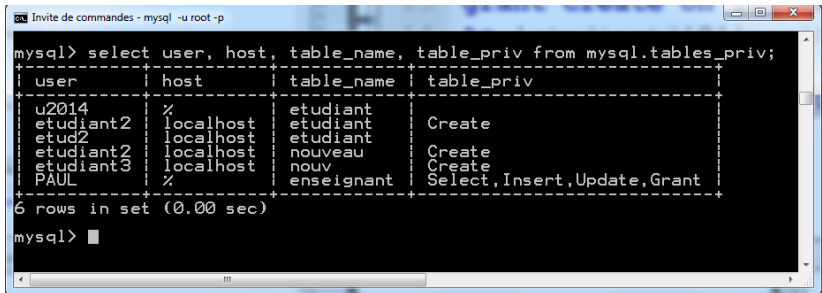
## Transmission de privilèges : WITH GRANT OPTION

- ▶ Il est possible de déclarer que les utilisateurs spécifiés dans la clause TO d'une commande GRANT peuvent eux-mêmes transmettre les privilèges (ou une partie de ceux-ci) à d'autres utilisateurs.
- ▶ Il faut terminer la commande GRANT avec WITH GRANT OPTION.
- ▶ Donnons à PAUL des privilèges sur la table ENSEIGNANT en lui permettant de les transmettre.

```
16 GRANT SELECT, INSERT, UPDATE ON  
17 ENSEIGNANT  
18 TO PAUL  
19 WITH GRANT OPTION;
```

## Transmission de privilèges : WITH GRANT OPTION

- Le privilège Grant représente le droit de retransmettre.



```
mysql> select user, host, table_name, table_priv from mysql.tables_priv;
```

user	host	table_name	table_priv
u2014	%	etudiant	
etudiant2	localhost	etudiant	Create
etud2	localhost	etudiant	
etudiant2	localhost	nouveau	Create
etudiant3	localhost	nouv	Create
PAUL	%	enseignant	Select, Insert, Update, Grant

```
6 rows in set (0.00 sec)
```

```
mysql> █
```

## Restriction des privilèges

- ▶ Il est aussi possible de fixer des restrictions d'utilisation à un utilisateur, par exemple combien de requêtes il peut soumettre à la base par heure.
- ▶ Donnons à JEAN le droit d'exécuter seulement une commande SELECT par heure.

```
1 GRANT SELECT
2 ON *
3 TO JEAN
4 WITH MAX_QUERIES_PER_HOUR 1
```

## Restriction des privilèges

En plus de `MAX_QUERIES_PER_HOUR`, il est possible de spécifier les restrictions

- ▶ `MAX_CONNECTIONS_PER_HOUR`
- ▶ `MAX_UPDATES_PER_HOUR`
- ▶ `MAX_USER_CONNECTIONS` (connexions simultanées).

## Révoquer les privilèges

Nous avons, ci-dessous, un exemple de révocation de privilège :

```
26 REVOKE INSERT, UPDATE ON
27 ENSEIGNANT
28 FROM PAUL;
```

Invite de commandes - mysql -u root -p

```
mysql> select user, host, table_name, table_priv from mysql.tables_priv;
```

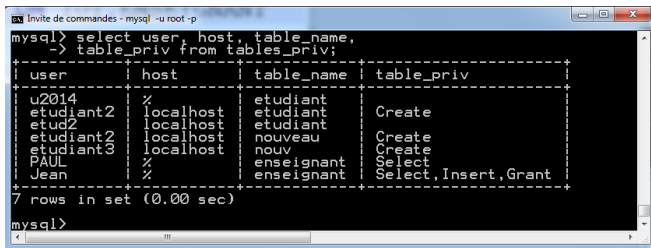
user	host	table_name	table_priv
u2014	%	etudiant	
etudiant2	localhost	etudiant	Create
etud2	localhost	etudiant	
etudiant2	localhost	nouveau	Create
etudiant3	localhost	nouv	Create
PAUL	%	enseignant	Select,Grant
Jean	%	enseignant	Select,Insert,Grant

```
7 rows in set (0.00 sec)

mysql> █
```

## Supprimer la transmission de privilèges

```
41 REVOKE GRANT OPTION ON IUT.ENSEIGNANT
42 FROM PAUL;
```



Invite de commandes - mysql -u root -p

```
mysql> select user, host, table_name,
-> table_priv from tables_priv;
```

user	host	table_name	table_priv
u2014	%	etudiant	
etudiant2	localhost	etudiant	Create
etud2	localhost	etudiant	
etudiant2	localhost	nouveau	Create
etudiant3	localhost	nouv	Create
PAUL	%	enseignant	Select
Jean	%	enseignant	Select, Insert, Grant

7 rows in set (0.00 sec)

```
mysql>
```



## Les tables de la base mysql

1. user
2. db
3. tables\_priv
4. columns\_priv
5. procs\_priv

## mysql.user

- ▶ Create\_priv : créer une table ou une base
- ▶ Drop\_priv : supprimer une table ou une base
- ▶ Index\_priv : créer ou supprimer un index
- ▶ Alter\_priv : modifier la structure d'une table, la renommer ou modifier une base (e.g. CHARACTER SET, COLLATION par défaut)

quelle que soit la base de données (excepté les bases système test et information\_schema).

## mysql.user

- ▶ Create\_user\_priv : créer (supprimer ou renommer) un utilisateur
- ▶ Grant\_priv : transmettre des droits qu'il aura lui-même reçus
- ▶ Show\_db\_priv : lister les bases de données existantes

quelle que soit la base de données.

## mysql.user

```
1  SELECT User,Host FROM mysql.user ;
2
3  #Privilèges objet (LMD) sur toutes les bases de données
4  SELECT Host, User,Select_priv, Insert_priv, Update_priv, Delete_priv
5  FROM mysql.user;
6
7  #Privilèges objet (LDD) sur toutes les bases de données
8  SELECT Host, User, Create_priv, Drop_priv,Index_priv, Alter_priv
9  FROM mysql.user;
10
11 #Privilèges système (LCD) sur toutes les bases de données
12 SELECT Host,User,Create_user_priv, Grant_priv, Show_db_priv
13 FROM mysql.user;
```

## mysql.user

```
14
15 #Privilèges à propos des vues sur toutes les bases de données
16 SELECT Host,User, Create_view_priv, Show_view_priv FROM mysql.user;
17
18 #Privilèges à propos des procédures cataloguées sur toutes les bases de données
19 SELECT Host,User,Create_routine_priv, Alter_routine_priv, Execute_priv
20 FROM mysql.user;
21
22 #Privilèges à propos des restrictions d'utilisateur
23 SELECT Host, User,max_questions "Requetes", max_updates "Modifs" ,
24 max_connections "Connexions", max_user_connections "Cx simult."
25 FROM mysql.user;
```

## mysql.db et mysql.columns\_priv

```
26
27 #Table mysql.db
28 SELECT Host, User, Db, Create_priv, Drop_priv, Alter_priv FROM mysql.db;
29
30 #Table mysql.columns_priv
31 SELECT CONCAT(User,'@',Host) "Compte", CONCAT(Db,'.',Table_name) "Objet",
32 Column_name, Column_priv FROM mysql.columns_priv;
33
34 #Table mysql.procs_priv
35
36 #Privilèges relatifs aux sous-programmes au niveau database.
37 SELECT CONCAT(User,'@',Host) "Compte", Db,
38 Create_routine_priv "create routine", Alter_routine_priv "alter routine",
39 Execute_priv "exec. routine" FROM mysql.db;
40
```

## mysql.procs\_priv et mysql.tables\_priv

```
41 # Privilèges relatifs aux sous-programmes au niveau routine.
42
43 SELECT CONCAT(User,'@',Host) "Compte",
44 CONCAT('.',Routine_name,':',Routine_type) "Objet",
45 Grantor, Proc_priv FROM mysql.procs_priv;
46
47 #Table mysql.tables_priv
48
49 SELECT CONCAT(User,'@',Host) "Compte",
50 CONCAT(Db,'.',Table_name) "Objet", Grantor, Table_priv
51 FROM mysql.tables_priv;
```

## Grant et vue

- ▶ Une commande GRANT peut faire référence non seulement à des tables, mais aussi à des vues.
- ▶ Il devient ainsi possible d'avoir des utilisateurs avec un accès à seulement
  1. une partie d'une table (e.g. projection, sélection), ou
  2. à des informations dérivées (e.g. calculs sur les colonnes) ou
  3. résumées des tables (e.g. regroupement, fonctions de groupe).

```
1 CREATE VIEW NOM_ADRESSE AS
2 SELECT NOM, INITIALES, RUE, NOMAISON, VILLE
3 FROM JOUEURS
4
5 GRANT SELECT
6 ON NOM_ADRESSE
7 TO DAVID
```



## Mot de passe root

- ▶ Mot de passe inexistant
- ▶ Mot de passe existant, lancer mysqld
  1. en utilisant un fichier : option `–init-file`
  2. sans utiliser un fichier : option `skip-grant-tables`

# Travaux pratiques

1. Mot de passs root
2. Privilèges
3. Accès distant

# References I