

Prof. DI Dr. Erich Gams

Datenmanipulation in SQL

Rechteverwaltung



informationssysteme htl-wels

To start....

Please, close your laptops



and just



Übersicht ➡ Was lernen wir?



- › Benutzerverwaltung in MySQL
- › Rechteverwaltung in MySQL
- › Rollen in MySQL

Erstellen eines neuen Benutzers

› Benutzer anlegen

```
CREATE USER 'benutzer'@'localhost' IDENTIFIED BY 'password';
```

‘username’@‘hostname’

‘username’@‘%example.com’

› Alle Benutzer anzeigen

```
select * from mysql.user;
```

Benutzer Rechte zuweisen

- › Einem Benutzer alle Rechte zuweisen.

```
GRANT ALL PRIVILEGES ON meineDB . * TO 'benutzer'@'localhost';
```

- › GRANT ALL PRIVILEGES
 - Es werden alle verfügbaren Privilegien (Rechte) zugewiesen.
- › ON ,meineDB' . *
 - Bereiche, auf die die Rechte zugewiesen werden sollen.
 - Möglich ist auch ,* . *', um einem Benutzer zum Beispiel alle Rechte einzuräumen
 - Einschränkung auf einzelne Tabellen einer Datenbank, wie z.B. "meineDB' . ,meineTabelle".
- › TO ,benutzer'@'localhost'
 - Der Benutzer, der diese Rechte erhalten soll.

Weitere Privilegien

- › **ALL PRIVILEGES**
 - Ein Wildcard für alle Rechte auf das gewählte Datenbankobjekt, mit einem *.* auf alle Datenbanken.
- › **CREATE, DROP**
 - Erlaubt einem Benutzer, Datenbanken zu erstellen bzw. zu löschen
- › **DELETE**
 - Erlaubt einem Benutzer, einzelne Zeilen in einer Tabelle zu löschen
- › **INSERT**
 - Erlaubt einem Benutzer, neue Zeilen in eine Tabelle zu schreiben
- › **SELECT**
 - Leseberechtigungen auf eine Datenbank oder Tabelle
- › **UPDATE**
 - Erlaubnis, eine Zeile zu aktualisieren
- › **GRANT OPTION**
 - Erlaubt einem Benutzer, die Rechte anderer Benutzer zu setzen oder zu widerrufen

Zusatz

- › Privilegien im Arbeitsspeicher upzudaten

```
FLUSH PRIVILEGES;
```

- › Privilegien anzeigen

```
SHOW GRANTS FOR 'benutzer'@'localhost';
```

- › Benutzer löschen

```
DROP USER 'benutzer'@'localhost';
```

Rollen

- › Rollen können Privilegien zugeteilt werden und Benutzer können Rollen zugeteilt und wieder entzogen werden.
- › 3 Rollen anlegen

```
CREATE ROLE 'app_developer', 'app_read', 'app_write';
```


Rollen Privilegien zuweisen

- › *app_developer* bekommt alle Rechte.
- › *app_read* bekommt nur Leserechte.
- › *app_write* kann Daten manipulieren.

```
GRANT ALL ON app_db.* TO 'app_developer';  
GRANT SELECT ON app_db.* TO 'app_read';  
GRANT INSERT, UPDATE, DELETE ON app_db.* TO 'app_write';
```

Privilegien an Benutzer weiterreichen

```
CREATE USER 'dev1'@'localhost' IDENTIFIED BY 'dev1pass';  
CREATE USER 'read_user1'@'localhost' IDENTIFIED BY 'read_user1pass';  
CREATE USER 'read_user2'@'localhost' IDENTIFIED BY 'read_user2pass';  
CREATE USER 'rw_user1'@'localhost' IDENTIFIED BY 'rw_user1pass';
```

```
GRANT 'app_developer' TO 'dev1'@'localhost';  
GRANT 'app_read' TO 'read_user1'@'localhost', 'read_user2'@'localhost';  
GRANT 'app_read', 'app_write' TO 'rw_user1'@'localhost';
```

Zusatz

- › Privilegien der Rolle *app_write* anzeigen

```
SHOW GRANTS FOR 'app_write';
```

- › Einem Benutzer die Rolle entziehen

```
REVOKE role FROM user;
```

- › Einer Rolle Privilegien entziehen

```
REVOKE INSERT, UPDATE, DELETE ON app_db.* FROM 'app_write';
```

- › Rollen löschen

```
DROP ROLE 'app_read', 'app_write';
```

›

Systemvariable setzen für Sichtbarkeit

› `set global activate_all_roles_on_login = ON`

Quellen

- › <https://gridscale.io/community/tutorials/mysql-benutzer-rechte-zuweisen/>
- › <https://dev.mysql.com/doc/refman/8.0/en/roles.html>
- › <https://gridscale.io/community/tutorials/mysql-feinabstimmung-benutzerrechte/>