

LU12A: Data Security & User Management (DCL) - Rollen & Berechtigungen

Lernziele (gemäss Bildungsplan) • Rollen/Berechtigungen vergeben (**GRANT/REVOKE**, Benutzer & Rollen verwalten) • **Datensicherheit/Datenschutz**: Prinzipien & schützenswerte Daten erkennen • MySQL-spezifische **DCL-Befehle** sicher anwenden



Voraussetzungen • MySQL 8.x, WebStorm mit DB-Plugin, Root-Verbindung vorhanden. • Achtung: Für Produktivsysteme nie mit root arbeiten – im Unterricht nutzen wir root **nur** zum Einrichten.

0) Kontext & Prinzipien

* **Least Privilege**: Jeder Account erhält nur die **minimal** benötigten Rechte. * **Trennung nach Aufgaben**: Lese-User (RO), Schreib-User (RW), Admin-User. * **Datenschutz**: Personenbezug erkennen (PII), Zugriff beschränken, Backups schützen.

1) Begriffe & Ebenen der Berechtigungen

Ebenen: Global → Schema → Tabelle → Spalte → Routine (PROCEDURE/FUNCTION). **Rollen** (MySQL 8): Mehrere Privilegien bündeln, **einmal** verwalten, **mehrfach** zuweisen. **Benutzer**: user '@'host (Host einschränken: localhost vs. % für extern).

2) Schritt-für-Schritt: Rollen & Benutzer anlegen



Ziel: Demo-Schema app_demo + Rollen app_read, app_write, app_admin + passende Benutzer. **Werkzeug**: WebStorm → Datenbank → SQL-Konsole (als root).

2.1 Demo-Schema & Tabelle

```
CREATE DATABASE IF NOT EXISTS app_demo;
USE app_demo;
```

```
CREATE TABLE IF NOT EXISTS notes(
  id INT PRIMARY KEY AUTO_INCREMENT,
  owner VARCHAR(64) NOT NULL,
  body TEXT
);
```

2.2 Rollen definieren

```
CREATE ROLE IF NOT EXISTS 'app_read', 'app_write',
'app_admin';
```

```
GRANT SELECT ON app_demo.* TO
'app_read';
GRANT SELECT, INSERT, UPDATE, DELETE ON app_demo.* TO
'app_write';
GRANT ALL PRIVILEGES ON app_demo.* TO
'app_admin';
```

2.3 Benutzer anlegen (lokal)

```
CREATE USER IF NOT EXISTS 'app_ro'@'localhost' IDENTIFIED
BY 'Str0ng!Ro';
CREATE USER IF NOT EXISTS 'app_rw'@'localhost' IDENTIFIED
BY 'Str0ng!Rw';
CREATE USER IF NOT EXISTS 'app_admin'@'localhost' IDENTIFIED
BY 'Str0ng!Admin';
```

2.4 Rollen zuweisen & Standardrolle setzen

```
GRANT 'app_read' TO 'app_ro'@'localhost';
GRANT 'app_write' TO 'app_rw'@'localhost';
GRANT 'app_admin' TO 'app_admin'@'localhost';

SET DEFAULT ROLE 'app_read' TO 'app_ro'@'localhost';
SET DEFAULT ROLE 'app_write' TO 'app_rw'@'localhost';
SET DEFAULT ROLE 'app_admin' TO 'app_admin'@'localhost';
```

2.5 Kontrolle

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

3) Test: Rollen wirken lassen

Als app_ro verbinden (neue Verbindung in WebStorm). Erwartung: SELECT [], INSERT/UPDATE/DELETE [].

3.1 Read-Only testen

```
-- als app_ro
USE app_demo;
SELECT * FROM notes;           -- sollte funktionieren
INSERT INTO notes(owner, body) VALUES ('lisa','hello'); --
-- sollte fehlschlagen (permission)
```

3.2 Rechte ändern (root)

```
-- als root
REVOKE 'app_write' FROM 'app_rw'@'localhost';
GRANT 'app_read' TO 'app_rw'@'localhost';
SHOW GRANTS FOR 'app_rw'@'localhost';
```

4) Feingranular & Sicherheit

Spaltenrechte

```
GRANT SELECT(id, owner) ON app_demo.notes TO
'app_ro'@'localhost';
```

Passwort-Policy & Ablauf

```
ALTER USER 'app_rw'@'localhost' PASSWORD EXPIRE INTERVAL 90
DAY;
ALTER USER 'app_rw'@'localhost' ACCOUNT LOCK;    -- bei
Bedarf
-- ALTER USER 'app_rw'@'localhost' ACCOUNT UNLOCK;
```

Benutzer & Hosts auflisten

```
SELECT USER, host FROM mysql.user ORDER BY USER, host;
```

5) Mini-Quiz (Kontrollfragen)

* Worin unterscheiden sich **WHERE** und **HAVING**? (Querbezug Aggregation + Rechteprüfung via SELECT) * Warum ist GRANT ALL ON *.* für App-User problematisch? * Was bedeutet user'@'localhost vs. user'@'%'? * Wie helfen **Rollen** bei späterem **Node/Express-Backend**?



Best Practice • Keine App unter root betreiben. • Host einschränken. • Rollen verwenden. • Passwörter rotieren. • Backups schützen (siehe **LU12B**). • Im Code mit **Prepared Statements** arbeiten (LU Backend).

From:
<https://wiki.bzz.ch/> - **BZZ - Modulwiki**

Permanent link:
https://wiki.bzz.ch/modul/m290_guko/learningunits/lu12/theorie/a_einfuerung?rev=1762892025

Last update: 2025/11/11 21:13

