

4.4 DCL

Sonntag, 10. September 2023 16:05



4.4 DCL

4.4 Data Control Language (DCL)

Ausgangssituation



Die Datenbank der KOSidas GmbH ist in Betrieb! Dies ist auch Ihr Verdienst. Jedoch ist den Mitarbeitern aufgefallen, dass jeder Mitarbeiter und jede Mitarbeiterin, egal aus welcher Abteilung, Zugriff auf alle Tabellen und Daten hat, sowie Datensätze nach Belieben löschen und anlegen kann. So konnten schon Mitarbeiter der Produktentwicklung durch ungünstige SQL-Anweisungen Kundendaten abrufen und diese sogar verändern.



Im Bereich der SQL-Datenbanken wird die Berechtigungsvergabe über die sogenannte **Data Control Language (DCL)** geregelt. Hierbei können nach Rollen und Nutzern bestimmte **Lese- und Schreibzugriffe** festgelegt werden.



Arbeitsauftrag

- a) Lassen Sie sich in Ihrem DBMS alle User mit dem Befehl

```
SELECT user FROM mysql.user;
```

 anzeigen.

- b) **Recherchieren** Sie die allgemeine Syntax zum **Anlegen** und **Löschen** eines neuen **Users**.

```
CREATE USER IF NOT EXISTS 'name'@'localhost'  
IDENTIFIED BY 'password';
```

```
DROP USER IF EXISTS 'name'@'localhost';
```

- c) **Legen** Sie nun **konkret den Nutzer** , KurtNagel' mit dem Passwort , 1234' an und betrachten Sie anschließend, welche Rechte er hat.

```
CREATE USER IF NOT EXISTS 'KurtNagel'@'localhost' IDENTIFIED BY '1234';
```

- d) Nun müssen dem neuen Nutzer nur noch entsprechende Rechte zugewiesen werden. **Informieren** Sie sich zunächst in Partnerarbeit über die Befehle zum **Vergeben** und **Entziehen von Rechten in SQL**. Vervollständigen Sie dazu die untenstehende Tabelle.

Rechte anzeigen	
SHOW GRANTS; SHOW GRANTS FOR 'user'@'host';	
Rechte vergeben	Rechte entziehen
GRANT [Liste Privilegien] ----- ON datenbank.tabelle TO user;	REVOKE [Liste Privilegien] ----- ON datenbank.tabelle FROM user;



Wenn man alle Tabellen
 einschließen will, dann ...

datenbank.*

Beispiele für Rechte (privileges)

SELECT, CREATE, INSERT, DELETE usw.

Wenn man nicht alle aufzählen
 will, geht auch ...

ALL PRIVILEGES

- e) **Vergeben** Sie an den **Nutzer , KurtNagel'** das Recht in der **datenbank** **nur Abfragen zu tätigen**.





Bei einem Nutzer scheint das noch alles einfach und schnell zu gehen. Was ist aber, wenn man mehrere Nutzer aus verschiedenen Abteilungen hat? Jedem Nutzer aus einer Abteilung immer wieder die gleichen Rechte zu geben ist eine große Tipparbeit. Es würde sich hier anbieten, wenn man gewisse Rechte kapseln könnte und diese dann den Nutzern zuweist. Dafür gibt es das Konzept der Rollen.

Rollen anlegen und löschen

```
CREATE ROLE [IF NOT EXISTS] 'rollenname'@'server';  
DROP ROLE [IF EXISTS] 'rollenname'@'server';
```



Arbeitsauftrag

- a) **Recherchieren** Sie, wie man Rollen Nutzern direkt **beim Anlegen** und **nachträglich zu weisen** kann.

Rollen beim Anlegen von Nutzern zuweisen

Rollen Nutzern nachträglich zuweisen



Das zuweisen von Rechten bei Rollen funktioniert analog zur Zuweisung bei Usern.

GRANT / REVOKE...
ON ...
TO [rolle] /
FROM [rolle]

- b) Legen Sie die Rolle „Rolle_Verkauf“ mit den Rechten SELECT auf alle Tabellen an. Zudem die Rechte UPDATE, DELETE und INSERT auf die Tabelle Kunde. Weisen anschließend die Rolle dem Nutzer , KurtNagel' zu.