

# LU09.A02 - SQL- DCL: CREATE USER

It is high time to mess a little around with our new SQL powers, don't you think? So, let's try it directly on our Webstorm.

As the database administrator, we want to create a new user and only grant this user the necessary rights to operate the web application, which includes DML operations such as INSERT, UPDATE, DELETE, but not DDL operations such as CREATE or DROP of tables. After all, we don't want the web application to take control over our database, are we?

## Requirements

- Work type: individual
- Timeframe: 10 Minutes
- Means of aid:
  - only teaching materials, no websearch, no use of ai.
  - Webstorm with connection to the MySQL-DB
- Expected result: Semantically and syntactically correct SQL statements according to the requirements of the case studies.

## Case studies / Assignments

As a database administrator we are assigned to create a `AppUser`, which has for security reasons only the right for DML operations, but must not be allowed for DDL operation. We don't want a hacker to delete our entire webshop, do we?

To get the job done, follow the instructions below:

1. Create as the `sysdba` (system administrator of the database) a new user
2. Grant this role only the necessary rights
3. Create as a `sysdba` a test table and fill it with some test data
4. Establish a new connection within the webstorm by using the credentials of this new user
5. Try out the DML operations, which should be possible (insert, update, delete)
6. Try out DDL operations, which should result in errors due to missing permissions for that particular user
7. Drop the newly created user finally

## Task A1

**Create the User:** Create a user named `restrictedUser` with the password `SafePassword123` using the `mysql_native_password` plugin.

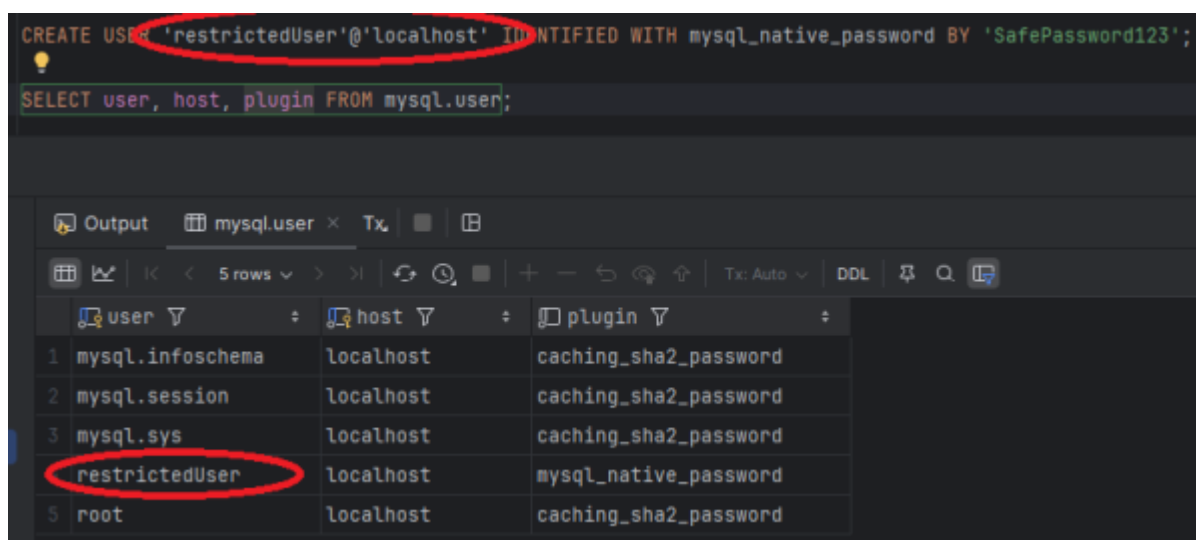
```
CREATE USER 'restrictedUser'@'localhost' IDENTIFIED WITH  
mysql_native_password BY 'SafePassword123';
```

## Task A2

**Overview of the current privileges:** Display all users.

```
SELECT user, host, plugin FROM mysql.user;
```

The result set should look like:



The screenshot shows a MySQL command-line interface. At the top, two SQL commands are entered: `CREATE USER 'restrictedUser'@'localhost' IDENTIFIED WITH mysql_native_password BY 'SafePassword123';` and `SELECT user, host, plugin FROM mysql.user;`. The first command is circled in red. Below the commands, the results of the `SELECT` query are displayed in a table. The table has three columns: `user`, `host`, and `plugin`. There are five rows of data. The row for `restrictedUser` is circled in red.

	user	host	plugin
1	mysql.infoschema	localhost	caching_sha2_password
2	mysql.session	localhost	caching_sha2_password
3	mysql.sys	localhost	caching_sha2_password
4	restrictedUser	localhost	mysql_native_password
5	root	localhost	caching_sha2_password

## Task A3

**Grant Privileges Without Table Management:** Grant the user *restrictedUser* the ability to read and write data but not to create, alter, or drop tables. Use the following commands to give only the required privileges.

```
GRANT SELECT, INSERT, UPDATE, DELETE ON myDatabase.* TO  
'restrictedUser'@'localhost';
```

## Task A4

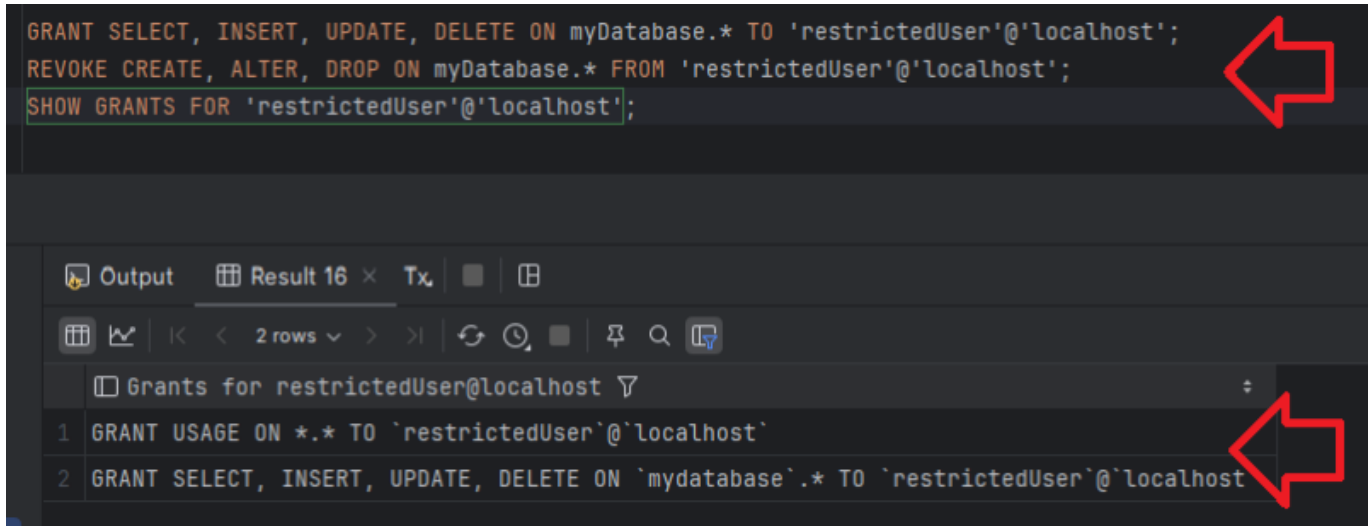
**Revoke Privileges:** To be certain that nothing unintended can happen revoke the CREATE, ALTER, and DROP privileges explicitly.

```
REVOKE CREATE, ALTER, DROP ON myDatabase.* FROM  
'restrictedUser'@'localhost';
```

## Task A5

**View the User's Privileges:** Check the privileges to ensure that the user cannot manage tables.

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



The screenshot shows a SQL IDE with a dark theme. The top panel displays the following SQL commands: `GRANT SELECT, INSERT, UPDATE, DELETE ON myDatabase.* TO 'restrictedUser'@'localhost';`, `REVOKE CREATE, ALTER, DROP ON myDatabase.* FROM 'restrictedUser'@'localhost';`, and `SHOW GRANTS FOR 'restrictedUser'@'localhost';`. The third command is highlighted with a green box. A red arrow points to the right from the first command. The bottom panel shows the output of the `SHOW GRANTS` command, titled "Grants for restrictedUser@localhost". It contains two rows: `1 GRANT USAGE ON *.* TO 'restrictedUser'@'localhost'` and `2 GRANT SELECT, INSERT, UPDATE, DELETE ON `mydatabase`.* TO 'restrictedUser'@'localhost'`. A red arrow points to the right from the second row.

## Task A6

**Test the User's Access:** Establish a new console connection to the database by using *restrictedUser* + *password* and try to perform a CREATE TABLE or DROP TABLE operation. The attempt should result in a permission error als displayed in the image below.

## Task A7

**Delete the User (optional):** After testing, you can delete the user if they are no longer needed.

## Solution

[Lösung](#)

## Vocabulary

English	German
explicitely	ausdrücklich
assignment	Auftrag
to revoke	widerrufen, aufheben



Volkan Demir

Last  
update: 2024/10/29 12:22 modül:m290:learningunits:lu06:aufgaben:a02 <https://wiki.bzz.ch/modul/m290/learningunits/lu06/aufgaben/a02?rev=1730200979>

---

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

Permanent link:  
<https://wiki.bzz.ch/modul/m290/learningunits/lu06/aufgaben/a02?rev=1730200979>

Last update: **2024/10/29 12:22**

