Data Control Language (DCL)

Database Design and Development
Cody Henrichsen
2020

3/22/21

Who gets access

- That is the question that the DCL subset is working to answer
- It works in both the positive and negative directions
- Most often the decision of management
- Themes
  - Structure
  - Security
  - Access

3/22/21

Who is involved

- Roles
  - Collective permission group
  - Very useful for business/academic not so for demo
  - Multiple memberships
    - Can have conflicting access levels
- Users
  - Individual level
  - password
  - IP/Host/Local

3/22/21

CREATE

- ▶ Normally part of DDL but users/roles fit here
- ▶ Define roles first, users after
  - ▶ Top down design
- ▶ HOST MATTERS!!!
- ▶ Specify password restrictions!

CREATE Syntax

CREATE ROLE

    role_name;

CREATE USER [IF NOT EXISTS]

    user_name

IDENTIFIED BY

    password

LIMITATIONS

PASSWORD OPTION;

```
CREATE ROLE
    administrati;
CREATE ROLE
    cs_teachers;

CREATE USER
    'lady_ada_lovelace'@'%'
IDENTIFIED BY
    'ultra_secure_pa5sw0rd'
WITH MAX_QUERIES_PER_HOUR
    47
PASSWORD EXPIRE
    INTERVAL 45 DAY;

CREATE USER IF NOT EXISTS
    'alan_turing'@'localhost'
IDENTIFIED BY
    'dead_password'
    'alan_turing'@'%'
IDENTIFIED BY
    'secure_password'
PASSWORD EXPIRE;
```

Privileges

- ▶ System Level
  - ▶ CREATE
  - ▶ DROP
  - ▶ ALTER
- ▶ Object Level
  - ▶ INSERT
  - ▶ SELECT
  - ▶ UPDATE
  - ▶ EXECUTE

GRANT

- Adds the specified permission(s) to the role / user
- Grouped by subset
- Can be applied on a user or role level
- Plan to give least access required at most common level and use roles to provide additional access as needed

---

GRANT Syntax

GRANT PRIVILEGE ON
    object
TO
    role

GRANT
    role
TO
    user

REVOKE

- If a permission is revoked from a user or role and a conflict results, the lower permission level is applied
- Can be applied to individual levels or ALL!
- Plan before use!

REVOKE Syntax

REVOKE PRIVILEGE ON

    structure

FROM

    user/role

REVOKE

    role

FROM

    user

```
REVOKE SELECT ON
    manga_fruit.*
FROM
    'anonymous_student'@'%';

REVOKE
    cs_teachers
FROM
    'hacked_account';
```

When???

- ▶ The DCL subset is generally for management level users of the database because of the data structure, privacy, and security concerns
- ▶ Not something that would be done or available to an entry level worker within the system
- ▶ Learn to read the errors when you get denied access to a resource

MariaDB permissions page

- ▶ Adds access to the database
  - ▶ Data group
    - ▶ DML
  - ▶ Structure group
    - ▶ DDL
  - ▶ Administration group
    - ▶ DCL