MariaDB Roles

Vicențiu Ciorbaru
Software Engineer @ MariaDB Foundation
How roles work in MariaDB
Roles in MariaDB

- Roles are similar to groups in the UNIX world

- A user can have one or more roles granted to them
  - GRANT developer_role TO user

- Only one role can be active at any one time.
  - SET ROLE developer_role
CREATE USER bob;
CREATE ROLE admin;
GRANT SELECT ON prod.statistics TO bob;
GRANT ALL ON on mysql.* to admin;
GRANT admin to bob;

SELECT * FROM prod.statistics;  # This works
SELECT user, password FROM mysql.user;
Error: Access denied to database mysql;

SET ROLE admin;
SELECT user, password FROM mysql.user;  # Now it works
Roles in MariaDB

- A role can have one or more roles granted to it.
  - No cycles!

GRANT
Roles in MariaDB

A role can have one or more roles granted to it.

CREATE ROLE reader;
CREATE ROLE writer;
CREATE ROLE reader_and_writer;
CREATE USER bob;

GRANT SELECT ON production.* TO reader;
GRANT UPDATE, INSERT, DELETE on production.* TO writer;

GRANT reader TO reader_and_writer;
GRANT writer TO reader_and_writer;

GRANT reader TO bob;
GRANT writer TO bob;
GRANT reader_and_writer TO bob;

<connect as bob>

SELECT * FROM production.data;  # Access denied.
SET ROLE reader;
SELECT * FROM production.data;  # Works.
INSERT (1) INTO production.data;  # Access denied.
SET ROLE writer;
INSERT (1) INTO production.data;  # Works
SELECT * FROM production.data;  # Access denied.
SET ROLE reader_and_writer;
SELECT * FROM production.data;  # Works
INSERT (1) INTO production.data;  # Access denied.
CREATE ROLE reader;
CREATE ROLE writer;
CREATE ROLE reader_and_writer;
CREATE USER bob;

GRANT SELECT ON production.* TO reader;
GRANT UPDATE, INSERT, DELETE ON production.* TO writer;

GRANT reader TO reader_and_writer;
GRANT writer TO reader_and_writer;

GRANT reader TO bob;
GRANT writer TO bob;
GRANT reader_and_writer TO bob;

- All privileges of a granted role belong to the grantee.
- Cycles are detected and are not allowed.
- We store the relations between roles and user grants in
  mysql.roles_mappings
Roles in MariaDB

Default Role (from MariaDB 10.1 onward)

- Old applications not aware of roles can't make use of them.
- A default role implies a SET ROLE call at connection time.
- DBAs can use roles to structure privileges for legacy applications.

```
CREATE ROLE admin;
CREATE USER bob;
GRANT ALL ON production.* TO admin;
GRANT admin TO bob;
SET DEFAULT ROLE admin FOR bob;
<connect as bob>
DROP TABLE production.credit_cards;
# Production is down :)
```
Roles in MariaDB

Roles can be queried in multiple ways:

- `SELECT user FROM mysql.user WHERE is_role='Y'
- `Information_schema.applicable_roles`
  - List of available roles to the current user.
- `Information_schema.enabled_roles`
  - See the current active role (or NULL if no role is set)
- `SHOW GRANTS [ FOR (user | role) ]`
Roles in MariaDB - Implementation

- Roles are stored entirely in memory
- Stored as a Directed Acyclic Graph (DAG)
- Both backwards and forward edges
- Manually implemented Depth First Search to avoid using up stack space
Thank You!

Contact me at:

vicentiu@mariadb.org
vicentiu@ciorbaru.io

Blogs:
mariadb.org/blog
vicentiu.ciorbaru.io