Creating Users/Roles

- Syntax (CREATE ROLE or CREATE USER):

```
CREATE ROLE [IF NOT EXISTS] role_name [WITH role_options];
```

  - `role_name`: Unique identifier (1-63 chars, alphanumeric + _/.).
  - `role_options`: e.g., LOGIN, PASSWORD 'secret', VALID UNTIL '2025-12-31'.
- Key Role Options:

Option	Description	Default
LOGIN	Enables login	NOLOGIN
CREATEROLE	Create/alter/drop roles	NOCREATEROLE
CREATEDB	Create/rename databases	NOCREATEDB
PASSWORD NULL	Certificate-only auth	None

- Examples:

-- Basic login user

```
CREATE USER maxroach WITH LOGIN PASSWORD 'securepass';
```

-- Non-login role for grouping

```
CREATE ROLE developers WITH NOLOGIN CREATEDB;
```

-- Cert-based user

```
CREATE ROLE certuser WITH LOGIN PASSWORD NULL SUBJECT 'CN=maxroach';
```

Altering Users/Roles

- Syntax (ALTER ROLE):

```
ALTER ROLE [IF EXISTS] role_name WITH role_option [, ...];
```

- Examples:

-- Enable login and set password

```
ALTER ROLE developers WITH LOGIN PASSWORD 'team123';
```

-- Disable password auth

```
ALTER ROLE maxroach WITH PASSWORD NULL;
```

-- Database-specific default

```
ALTER ROLE maxroach IN DATABASE movr SET timezone = 'America/New_York';
```

-- For all roles

```
ALTER ROLE ALL SET sql_safe_updates = false;
```

Viewing Users/Roles

- Syntax (SHOW ROLES):

```
SHOW ROLES;
```

- Lists all roles with options, members, and last login.

- Related Commands:

```
- `SHOW GRANTS ON ROLE role_name;` - View role memberships.
- `SHOW GRANTS;` - View object privileges.
```

- Example Output:

```
> SHOW ROLES;
 username | options        | member_of | last_login
---------+---------------+-----------+------------
 admin    | {CREATEROLE}   | {}         | NULL
 max      | {LOGIN}        | {admin}    | 2025-11-17
```

(2 rows)

- Tip: Use `SHOW GRANTS ON ROLE developers FOR max;` to check specific grants.

Dropping Users/Roles

- Syntax (DROP ROLE):

```
DROP ROLE [IF EXISTS] role_name [, ...];
```

- Revoke all privileges first; cannot drop if members exist.

- Prerequisites:

```
  - Revoke privileges: `REVOKE ALL ON * FROM role_name;`
  - Revoke memberships: `REVOKE role_name FROM members;`
```

- Example:

-- Check grants

```
SHOW GRANTS ON documents FOR dev_ops;
```

-- Revoke

```
REVOKE INSERT ON documents FROM dev_ops;
```

-- Drop

```
DROP ROLE dev_ops;
```

- Warning: Cannot drop `root` or `admin`; use `IF EXISTS` to avoid errors.

Granting Role Membership

- Syntax (GRANT role TO user):

```
GRANT role_name TO role_spec [, ...] [WITH ADMIN OPTION];
```

- Adds users/roles as members; inherits privileges.

- Requirements: Granter must be role admin or in `admin` role.

- Examples:

-- Basic membership

```
GRANT developers TO maxroach;
```

-- With admin rights

```
GRANT developers TO maxroach WITH ADMIN OPTION;
```

-- Verify

```
SHOW GRANTS ON ROLE developers;
```

- Benefit: Simplifies privilege management – grant once to role, add users to it.

Revoking Role Membership

- Syntax (REVOKE role FROM user):

```
REVOKE role_name [ADMIN OPTION] FROM role_spec [, ...];
```

 - Removes membership or just admin option.
- Requirements: Granter must be role admin.
- Examples:

-- Remove membership

```
REVOKE developers FROM maxroach;
```

-- Revoke only admin option

```
REVOKE ADMIN OPTION FOR developers FROM maxroach;
```

- Note: Inherited privileges are revoked immediately; no loops allowed.

Granting Privileges

- Syntax (Grant Privileges):

```
GRANT {ALL | privilege_list} ON grant_target TO role_spec [WITH GRANT OPTION];
```

 - Targets: DATABASE, TABLE, SCHEMA, etc.
- Common Privileges: SELECT, INSERT, UPDATE, DELETE, CREATE, ZONECONFIG.
- Examples:

-- All on database

```
GRANT ALL ON DATABASE movr TO developers;
```

-- Specific on table

```
GRANT SELECT, INSERT ON TABLE rides TO maxroach WITH GRANT OPTION;
```

-- All future tables

```
ALTER DEFAULT PRIVILEGES FOR ROLE admin GRANT SELECT ON TABLES TO public;
```

Revoking Privileges

- Syntax (REVOKE Privileges):

```
REVOKE {ALL | privilege_list} ON grant_target FROM role_spec;
```

  - Applies to objects or system.
- Requirements: Granter needs GRANT OPTION on the privilege.
- **Examples:**

-- All on table

```
REVOKE ALL ON TABLE rides FROM maxroach;
```

-- Specific system

```
REVOKE CREATEROLE ON SYSTEM FROM developers;
```

-- All in schema

```
REVOKE ALL ON ALL TABLES IN SCHEMA public FROM maxroach;
```

- Note: Does not cascade to inherited privileges – revoke directly if needed.