Data object privileges

Learning Objectives

▶ Data governance model

▶ Managing Permissions for Data objects

Data governance model

▶ Programmatically grant, deny, and revoke access to data objects

GRANT Privilege **ON** Object <object-name> **TO** <user or group>

▶ **GRANT** <u>**SELECT**</u> **ON** <u>**TABLE**</u> my_table **TO** user_1@company.com

Data objects

GRANT Privilege **ON** Object <object-name> **TO** <user or group>

| Object	Scope
CATALOG	controls access to the entire data catalog.
SCHEMA	controls access to a database.
TABLE	controls access to a managed or external table.
VIEW	controls access to SQL views.
FUNCTION	controls access to a named function.
ANY FILE	controls access to the underlying filesystem.

Privileges

GRANT Privilege **ON** Object <object-name> **TO** <user or group>

Privilege	Ability
SELECT	read access to an object.
MODIFY	add, delete, and modify data to or from an object.
CREATE	create an object
READ_METADATA	view an object and its metadata.
USAGE	No effect! required to perform any action on a database object.
ALL PRIVILEGES	gives all privileges

Granting Privileges by Role

Role	Can grant access privileges for
Databricks administrator	All objects in the catalog and the underlying filesystem.
Catalog owner	All objects in the catalog.
Database owner	All objects in the database.
Table owner	Only the table
…	…

```
          Catalog
             |
          Schema
        (Database)
       /     |      \
   Table    View    Function
```
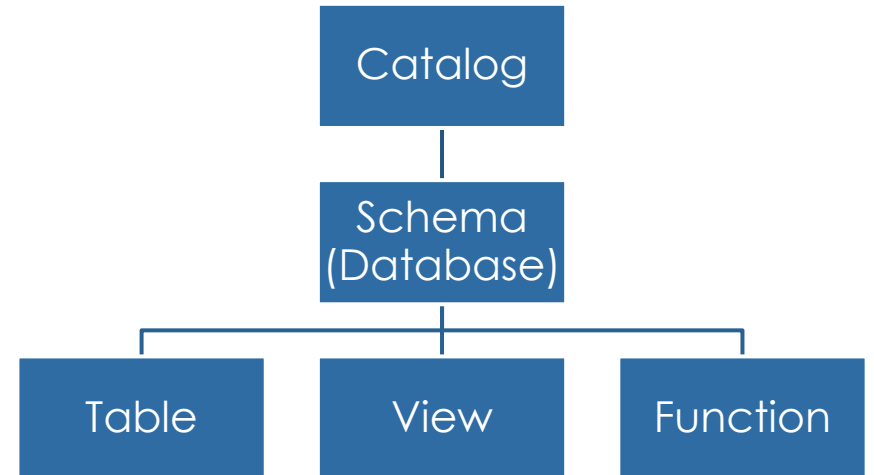
More operations

▶ Grant

▶ DENY

▶ REVOKE

▶ SHOW GRANTS