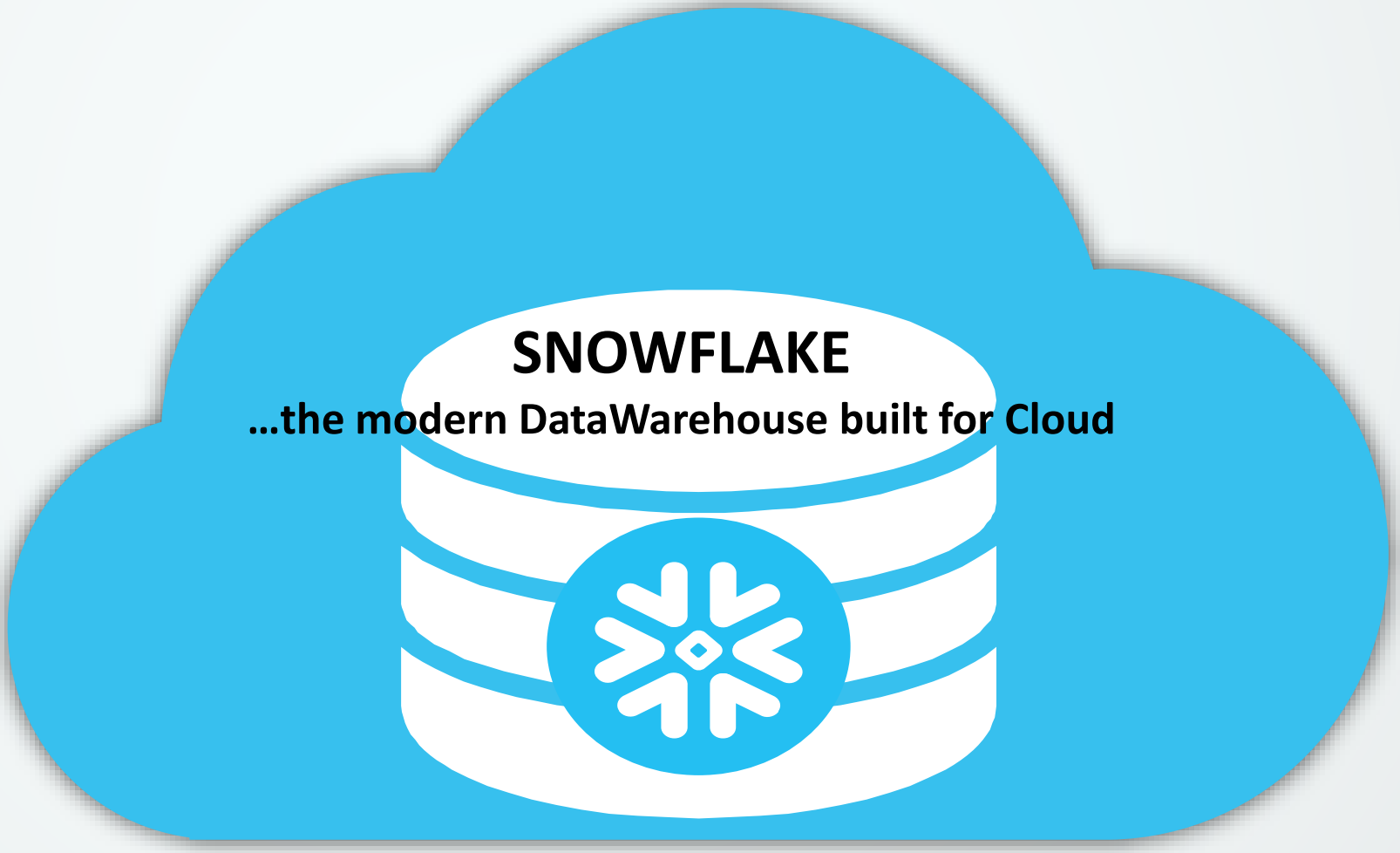


“Simplicity is the ultimate sophistication”

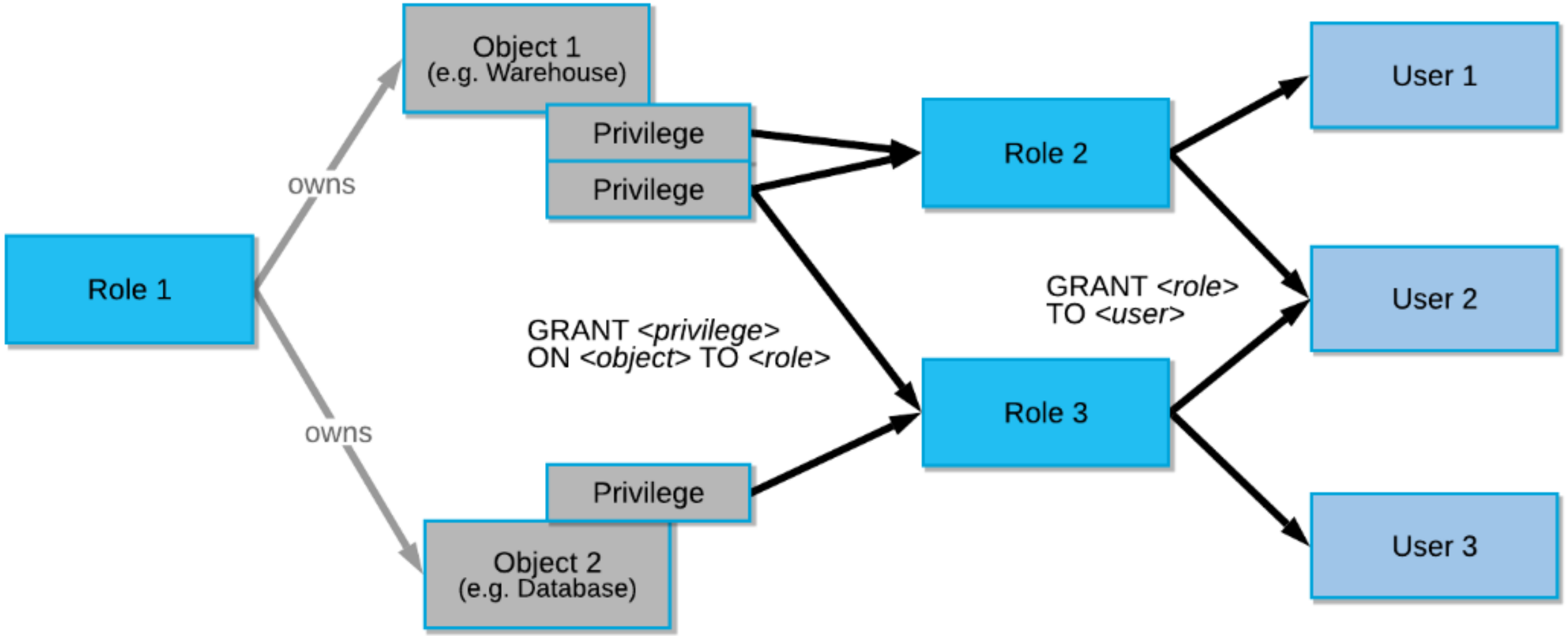
Leonardo da Vinci

Day-4

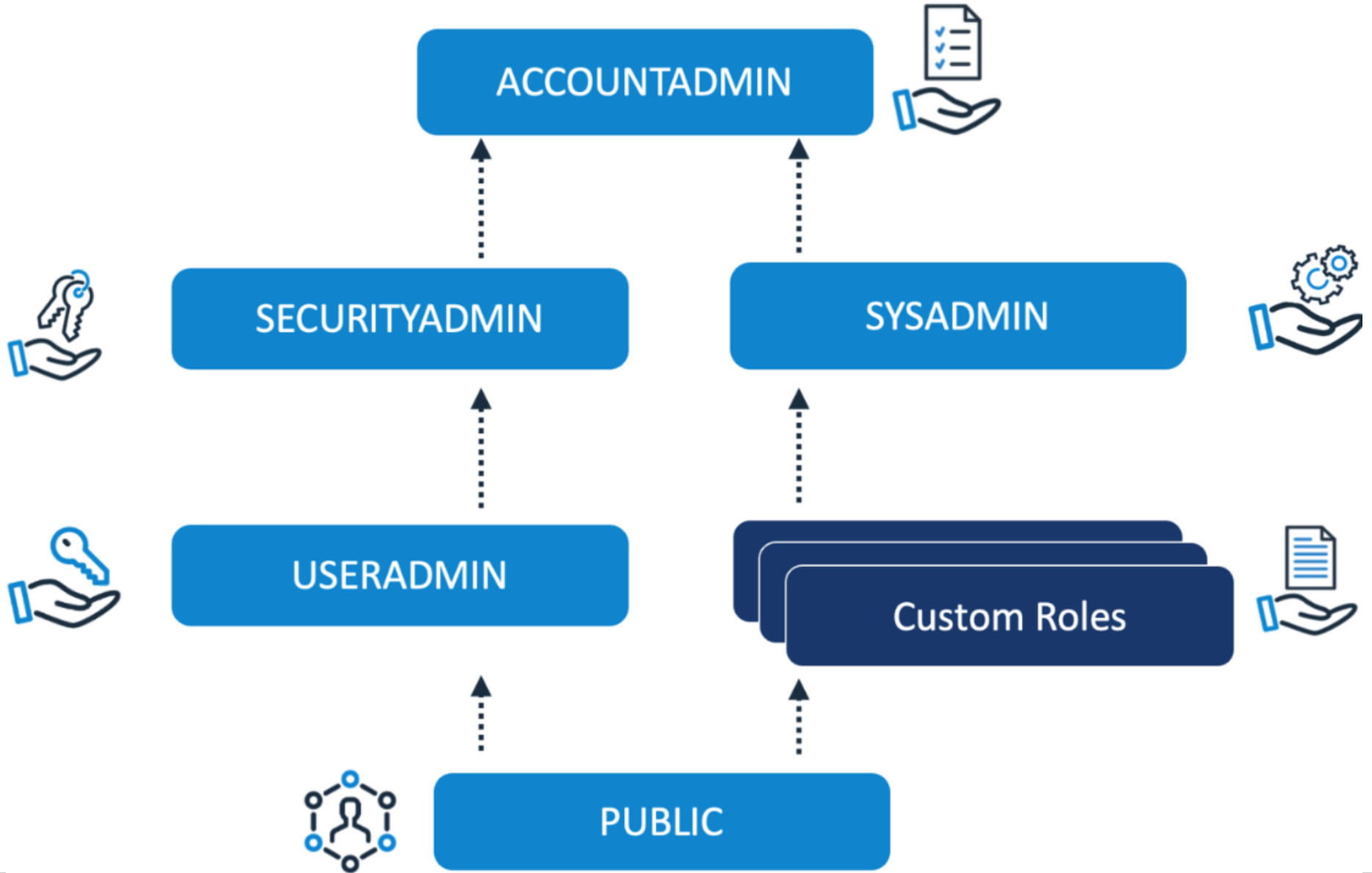
Access Control Model

- ❑ Discretionary Access Control (DAC)
  - ✓ Determine access
  - ✓ Grant access
  - ✓ Audit access
  - ✓ Revoke access
  - ✓ Prevent access
- ❑ Role-based Access Control (RBAC)

Security and Access Control

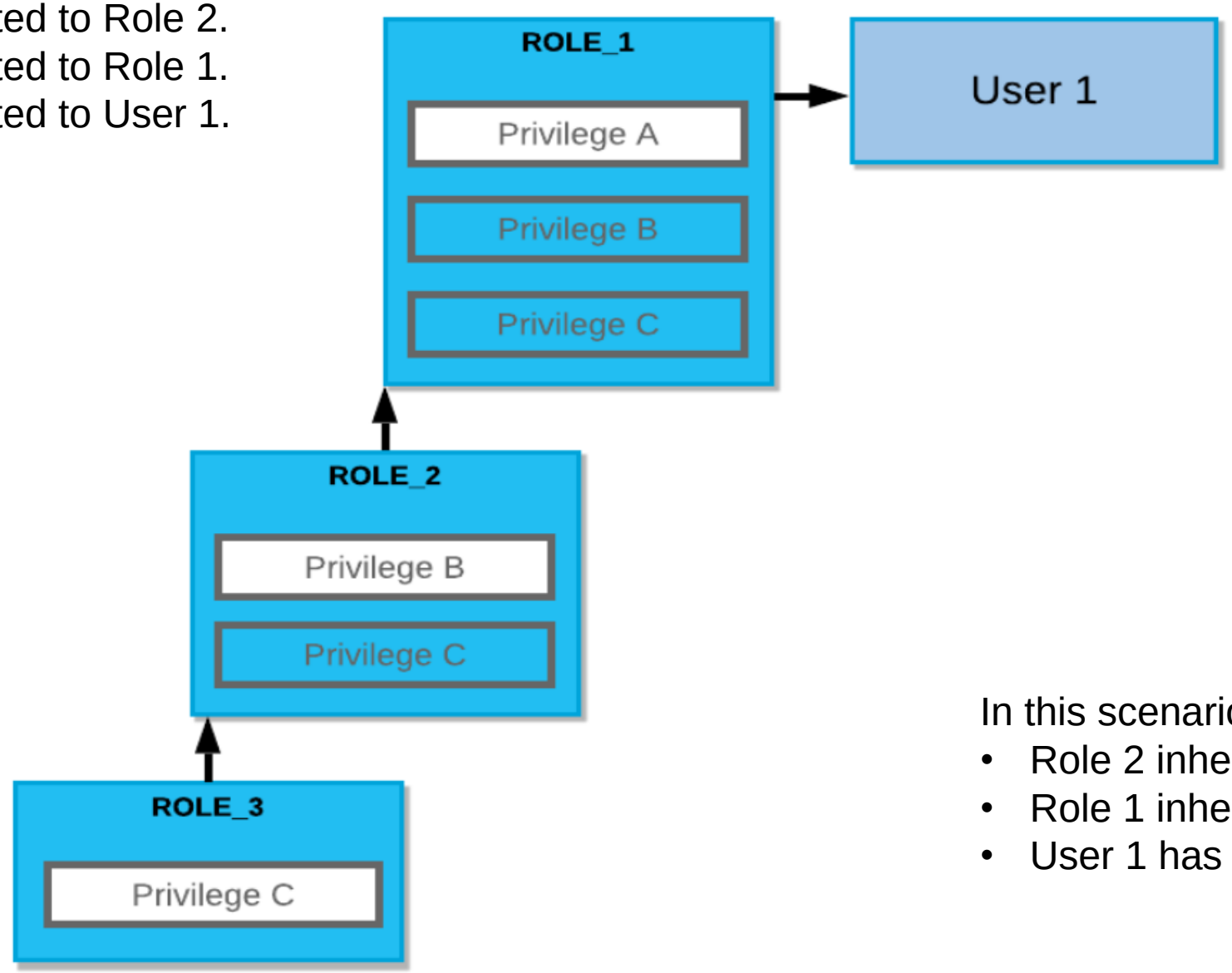


Security and Access Control



Security and Access Control

- Role 3 has been granted to Role 2.
- Role 2 has been granted to Role 1.
- Role 1 has been granted to User 1.



In this scenario:

- Role 2 inherits Privilege C.
- Role 1 inherits Privileges B and C.
- User 1 has all three privileges.

Access Control Privileges

- Global Privileges
- Account Privileges
- Schema Privileges
- Object Privileges
- Future Privileges

Object Privileges

DATABASE Privileges

Privilege	Usage
MODIFY	Enables altering any settings of a database.
MONITOR	Enables performing the DESCRIBE command on the database.
USAGE	Enables using a database. Additional privileges are required to view or take actions on objects in a database.
CREATE SCHEMA	Enables creating a new schema in a database, including cloning a schema.
IMPORTED PRIVILEGES	Enables roles other than the owning role to access a shared database; applies only to shared databases.
ALL [PRIVILEGES]	Grants all privileges, except OWNERSHIP, on a database.
OWNERSHIP	Transfers ownership of a database, which grants full control over the database.

Object Privileges

SCHEMA Privileges

Privilege	Usage
MODIFY	Enables altering any settings of a schema.
MONITOR	Enables performing the DESCRIBE command on the schema.
USAGE	Enables using a schema, including executing SHOW <OBJECT>
CREATE TABLE	Enables creating a new table in a schema, including cloning a table.
CREATE EXTERNAL TABLE	Enables creating a new external table in a schema.
CREATE VIEW	Enables creating a new view in a schema.
CREATE MATERIALIZED VIEW	Enables creating a new materialized view in a schema.
CREATE MASKING POLICY	Enables creating a new Column-level Security masking policy in a schema.
CREATE STAGE	Enables creating a new stage in a schema, including cloning a stage.
CREATE FILE FORMAT	Enables creating a new file format in a schema, including cloning a file format.
CREATE SEQUENCE	Enables creating a new sequence in a schema, including cloning a sequence.

Object Privileges

SCHEMA Privileges

Privilege	Usage
CREATE FUNCTION	Enables creating a new UDF or external function in a schema.
CREATE PIPE	Enables creating a new pipe in a schema.
CREATE TASK	Enables creating a new task in a schema, including cloning a task.
CREATE PROCEDURE	Enables creating a new stored procedure in a schema.
ALL [PRIVILEGES]	Grants all privileges, except OWNERSHIP, on a schema.
OWNERSHIP	Transfers ownership of a schema, which grants full control over the schema.

Object Privileges

TABLE Privileges

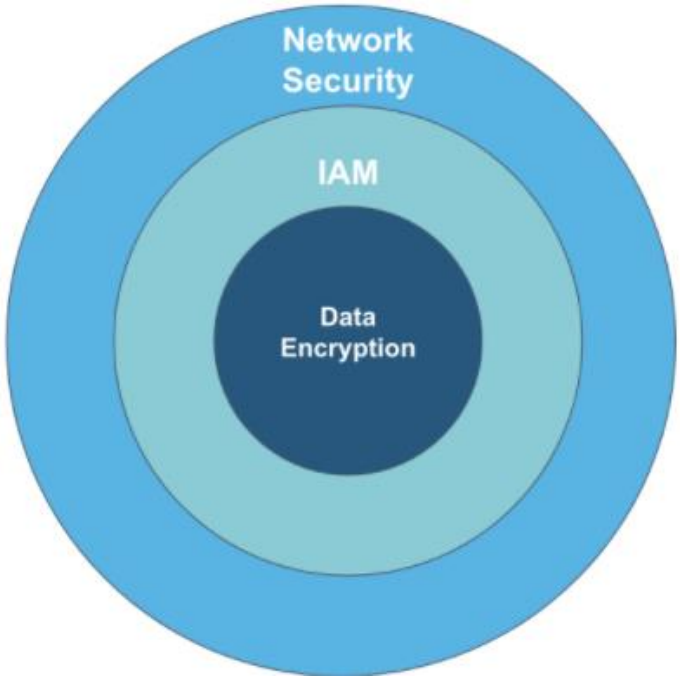
Privilege	Usage
SELECT	Execute a SELECT statement on the table.
INSERT	Execute an INSERT command on the table.
UPDATE	Execute an UPDATE command on the table.
TRUNCATE	Execute a TRUNCATE command on the table.
DELETE	Execute a DELETE command on the table.
REFERENCES	Reference the table as the unique/primary key table for a foreign key constraint.
ALL [PRIVILEGES]	Grant all privileges, except OWNERSHIP, on the table.
OWNERSHIP	Grant full control over a table.

Security Best Practices

Snowflake secures customer data using 3 layers

Network security or isolation provides the first line of defense. The network security best practices are as follows:

- Use network policies
- Use private connectivity with Snowflake.
- Allow firewall to connect client applications to Snowflake.
- Allow Snowflake to access your cloud storage location for loading/unloading data.



IAM : Once your Snowflake account is accessible, the next step in gaining access to Snowflake is to authenticate the user. Users must be created in Snowflake prior to any access. Once the user is authenticated, a session is created with roles used to authorize access in Snowflake.

- Managing users and roles
- Authentication and single sign-on
- Sessions
- Object-level access control (authorization)
- Column-level access control
- Row-level access control.

Data Encryption : The data encryption best practices are as follows:

- Use Tri-Secret secure and review AWS Tri-Secret Secure and Azure Tri-Secret Secure FAQs
- Use automatic key rotation for the CMK as provided by the cloud provider (such as AWS KMS). If, for any reason, you need to manually change your CMK, then contact Snowflake support for assistance.
- Remember to enable Tri-Secret Secure in the target account when using the Replication feature to replicate a database to another account.
- Enable periodic rekeying in Snowflake if your organization requires rekeying of data at regular intervals.
- If you want to encrypt/decrypt certain columns in addition to the transparent encryption provided by Snowflake, then use the built-in encryption functions.

Time Travel + Fail Safe

Time Travel + Fail Safe

Continuous Data Protection Lifecycle

Standard operations allowed:
Queries, DDL, DML, etc.

Time Travel allowed:
`SELECT … AT|BEFORE …`
`CLONE … AT|BEFORE …`
`UNDROP …`

No user operations allowed
(data recoverable only by Snowflake)

Snowflake Table Types

- Permanent Table
- Transient Table
- Temporary Table
- External Table

Snowflake Table Types

Type	Persistent	Time Travel Retention Period (Days)	Fail-safe Period (Days
Temporary	Remainder of session	0 or 1 (Default is 1)	0
Transient	Until explicitly dropped	0 or 1 (Default is 1)	0
Permanent (Standard Edition)	Until explicitly dropped	0 or 1 (Default is 1)	7
Permanent (Enterprise Edition and higher)	Until explicitly dropped	0 to 90 (Default is configurable)	7

Table Creation Demo