Query Lifecycle
Unity Catalog Security Model

1. Send query
2. Check namespace, metadata and grants
3. Assume IAM Role or Service Principal
4. Return short-lived token and signed URL
5. Request data from URL with short-lived token
6. Return data
7. Enforce policies

Principal — Compute — unity catalog — Audit Log — Cloud Storage

---
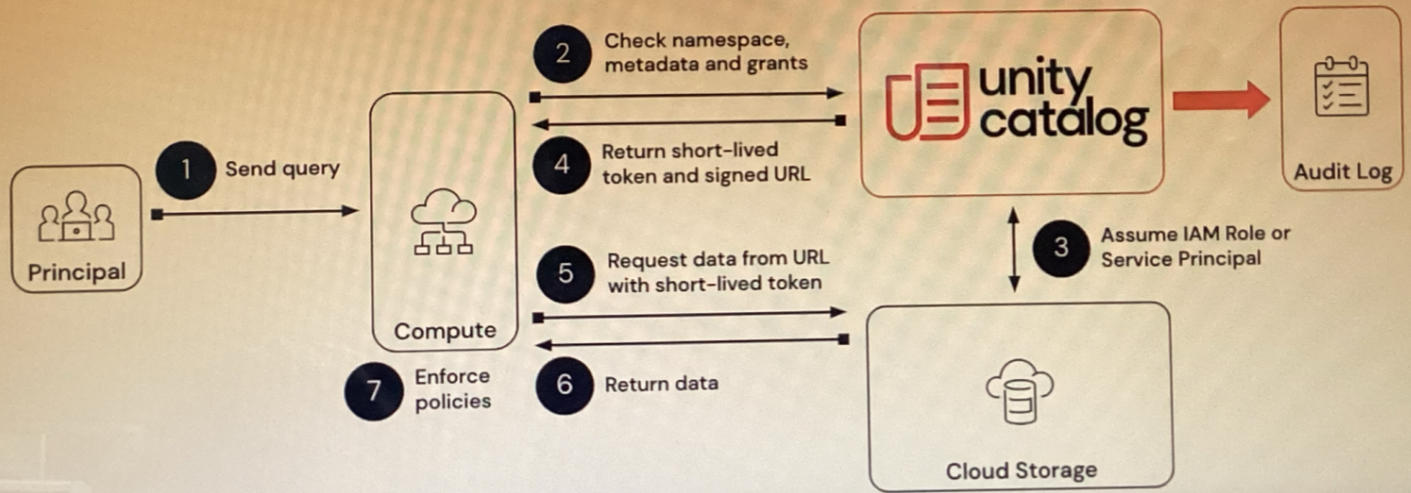
❯ When Unity Catalog is implemented, the Compute before directly accessing the data from the cloud, 1st, it sends the query to Unity Catalog.

❯ The Unity Catalog then checks the objects that are tried to be accessed, against the credentials provided for access.
Also, it logs that what objects are being accessed, when, and by whom.

❯ After verification of the credentials, UC returns a short-lived token and URL to the compute.
Using that token and URL, compute requests

data from the cloud storage, and if it matches, data is successfully returned.

This request process, of creds-verification, URL & token generation, and access using it, is repeated for each database object in the query.