Create and Update Data Role

Data Roles in Snowflake Environment

Overview:

Data roles serve as the foundational tier for accessing data within our Snowflake environment. They determine the access level for various database components such as databases, schemas, tables, and views. These roles not only specify permissions for existing components but also set permissions for future entities.

Creation & Management:

Automated Process:

The process of creating data roles has been streamlined through automation. The creation of these roles is facilitated using a dbt macro, ensuring efficiency and consistency.

All Snowflake Administrator have the authorization to:

- Create a new data role.
- Update an existing data role.
- Drop a data role.

Deployment & Oversight:

Approval Process:

To maintain the integrity and security of our Snowflake environment, all data roles undergo a strict review process before being deployed to the production environment. The Snowflake administrator holds the responsibility of:

- Ensuring that a Jira ticket was created and includes:
  Purpose, Use Cases, and Business Value: Clearly state the reasons for requesting the data role, how it will be used, and the expected business benefits.
- **Environment Selection**: Specify the target environment - either Non PROD or PROD.
- **Data Specification**: Enumerate the databases, schemas, tables and/or views that you'd like to be included in the data role.
- Reviewing each data role.
- Approving it for production deployment.

This process ensures that data access permissions align with organizational best practices and data security standards.

> ℹ️ Always follow organizational policies and guidelines when interacting with or managing data roles.

Code

Data Roles, Functional Roles, Service Roles with their permissions are defined in the package `dbt_bussys` macro(s) `macros/security/config_security_<envir>.sql`

The logic of the dictionary follow the below rules:

```
1    "ROLE_NAME": {
2        "comment":"ROLE_DESCRIPTION",
3        "database": ["DATABASE1","DATABASE2"],
4        "schemas": [
5            {
6                "name": "DATABASE1.SCHEMA",
7                "future": "YES",
8                "table": ["DATABASE1.SCHEMA.TBL1","DATABASE1.SCHEMA.TBL2"],
9                "view": ["DATABASE1.SCHEMA.VW1,DATABASE1.SCHEMA.VW2"]
10           },
11           {
12               "name": "DATABASE2.SCHEMA",
13               "future": "NO",
14               "table": ["ALL"],
15               "view": ["NA"]
16           }
17       ],
18       "is_active": "YES",
19   }
```

Objects	Sample Value	Definition

ROLE_NAME	PRD_SALESFORCE_ALL_DR	Name of the data role.
		Naming convention: <Environment>_<Source>_<Type>_DR
		<Environment> = PRD or HRD or QA or DEV
		<Source> = name of the data source i.e. Salesforce or Netsuite
		<Type> = data privacy where:
		        ALL = PII and non PII data
		        PII = PII data only

COMMENT	Data Role to read All Raw Totango data used by AX data sharing.	Plain English description of the role.
DATABASE	["RAW_PRD","PROD_DB"]	List of database(s) to grant usage to the role
SCHEMAS.NAME	RAW_PRD.SALESFORCE	List of schema(s) to grant usage to the role. ⚠ ALL can be used instead of a schema name. It will grant usage on all schemas in the database and future schemas in the database.
SCHEMAS.FUTURE	YES or NO	If NO, grant select to current tables and views listed in SCHEMAS.TABLE and in SCHEMAS.VIEW. if YES, in addition to grant select to current tables and views listed in SCHEMAS.TABLE and in SCHEMAS.VIEW, grant select on future tables and views in SCHEMAS.NAME

SCHEMAS.TABLE	["RAW_PRD.SALESFORCE.ACCOUNT", "RAW_PRD.SALESFORCE.ACCOUNT_TEAMMEMBER", "RAW_PRD.SALESFORCE.ASSIGNMENT"]	List of table(s) to grant select to the role. Enter ["NA"] if no tables will be granted select to the role. ⚠️ ["ALL'] can be used instead of a table name. It will grant select on all tables in schema.
SCHEMAS.VIEW	["PROD_DB.BASE_SALESFORCE.BASE_ACCOUNT","PROD_DB.BASE_SALESFORCE.BASE_ACCOUNT"]	List of views(s) to grant select to the role. Enter ["NA"] if no views will be granted select to the role. ⚠️ ["ALL'] can be used instead of a view name. It will grant select on all views in schema.
IS_ACTIVE	YES or NO	If YES, the role will be created or the updated permission will be assigned to the role. If NO, the role will be dropped.