RBAC Setup (Along with Database/Schema creation)

Database Creation Process:

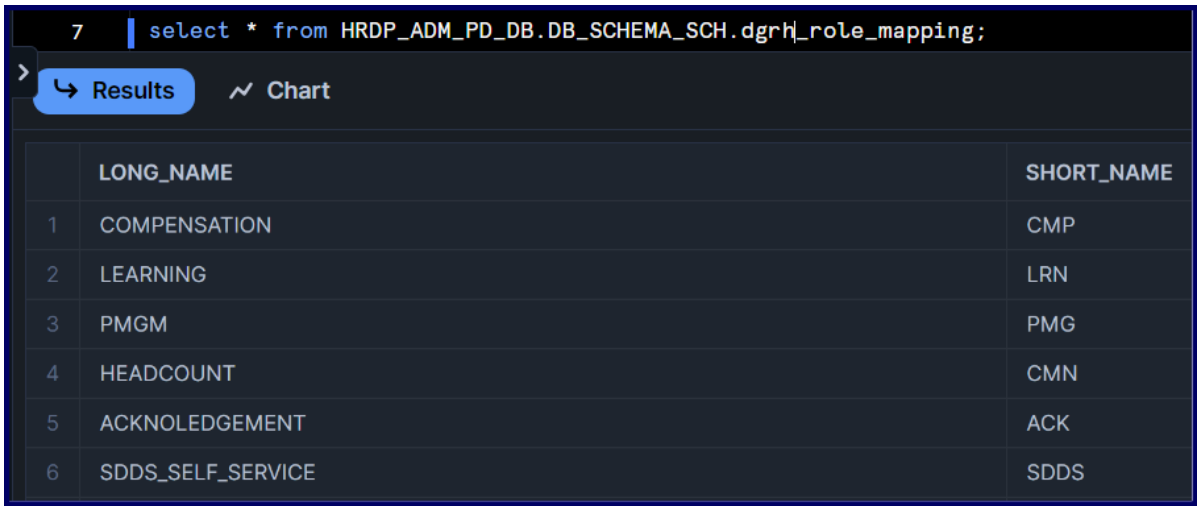
1. Use HRDP_DB_ADMIN_ROLE role to execute this step.
2. Execute HRDP_ADM_PD_DB.DB_SCHEMA_SCH.CREATE_DATABASE_SP('*<Database Name>*').
3. Database/Schema Naming Convention: *Database name should be like HRDP_XXX_PD_DB for Production*, Here "XXX" is like LND/STG/CORE /PUB etc..

Schema Creation Process:

1. Use HRDP_PD_DOMAIN_ADMIN role (equivalent environment admin for lower environment). You can run using DBT Infra project too as that will be having environment admin.
2. Execute HRDP_ADM_PD_DB.DB_SCHEMA_SCH.CREATE_SCHEMA_SP('*<Database Name>', '<Schema Name>*'). If database doesn't exist it will fail the process.
3. Database/Schema Naming Convention:
    a. *Database name should be like HRDP_XXX_PD_DB for Production*, Here "XXX" is like LND/STG/CORE/PUB etc..
    b. *Schema name should be ending with SCH*, *For SDDS database there will be exception for Schema name where we need to have as BTDP DS_C1_H01_XXXXXXXXX_PD/PD_PRIVATE*

DGRH Role Access Setup *(When new subject area added)***:**

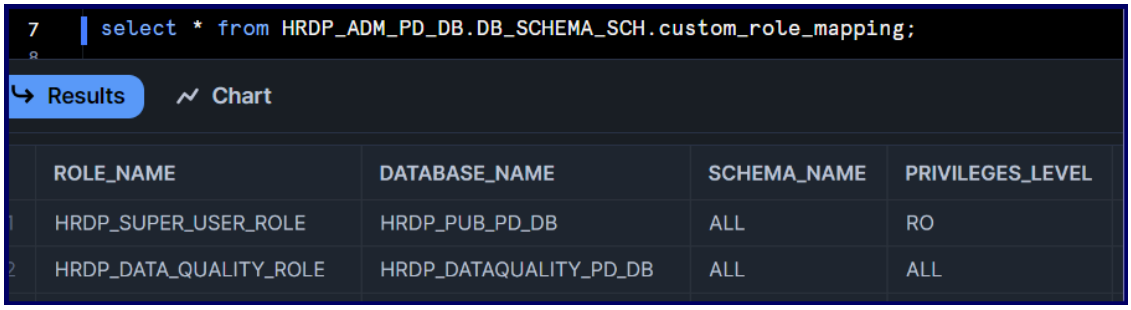
1. Insert an entry with Long Name and Short Name combination into git seed file (*infra/dbt/seeds/adm/dgrh_role_mapping_seed.csv*) and merge to corresponding environment. Ex: COMPENSATION as CMN
2. Rest everything will automatically take care (starting from loading table and till execution of procedure to provide access).
3. Please note that DGRH roles should have naming conventions like DGRH-PAPLATFORM-*<Long Name>*-*<Environment>*. Environment values are DEV, QUAL, NP and PRD.
4. Also note that this process is set for Publish Database access by subject domain.



	LONG_NAME	SHORT_NAME
1	COMPENSATION	CMP
2	LEARNING	LRN
3	PMGM	PMG
4	HEADCOUNT	CMN
5	ACKNOLEDGEMENT	ACK
6	SDDS_SELF_SERVICE	SDDS

Custom Role Access Setup:

1. Insert an entry into git seed file (*infra/dbt/seeds/adm/custom_role_mapping_seed.csv*) with Role Name, Database Name, Schema Name ('All' if whole database access needed) and Privilege level (ALL, RW and RO).
2. Rest everything will automatically take care (starting from loading table and till execution of procedure to provide access).



	ROLE_NAME	DATABASE_NAME	SCHEMA_NAME	PRIVILEGES_LEVEL
1	HRDP_SUPER_USER_ROLE	HRDP_PUB_PD_DB	ALL	RO
2	HRDP_DATA_QUALITY_ROLE	HRDP_DATAQUALITY_PD_DB	ALL	ALL

Notes: Refer HRDP_ADM_PD_DB.DB_SCHEMA_SCH.*ROLE_DAR_MAPPING* table to check when which role is granted with which DAR.

KT Recording: Discussion on New Schema Creation and Custom Role Setup-20240917_180342-Meeting Recording.mp4

Few more details of New Database/Schema creation with RBAC:

1. **Create Database:**

    a. Procedure Details: HRDP_ADM_PD_DB.DB_SCHEMA_SCH.CREATE_DATABASE_SP(DATABASE_NAME varchar)
    b. This process will create new database if not exists.
    c. Grant ALL privilege for specific database to Environment Admin, In special case to Data Quality group too. This will allow admin to create schema and anything they want in the database.
    d. Finally record the Database Name into DATABASE_TABLE table for reference.
2. **Create Schema, Database Access Role (DAR) with grants to default roles:**
    a. Procedure Details: HRDP_ADM_PD_DB.DB_SCHEMA_SCH.CREATE_SCHEMA_SP(DATABASE_NAME varchar, SCHEMA_NAME varchar)
    b. This process will create new new schema if not exists.
    c. All object ownership will be with environment admin role (HRDP_PD_DOMAIN_ADMIN) or specific owner role.
    d. This process will create 3 types (ALL, RW & RO) of Database Access Roles (DAR) at Database and Schema level. For detail understanding please refer RBAC Architecture.
    e. Database level DAR Naming convention is followed as DAR_<Ref Database Name>_ALL/RW/RO.
    f. Schema level DAR Naming convention is followed as DAR_<Ref Database Name>_<Ref Schema name>_ALL/RW/RO and same will be aggregated to Database level DARs. *Exceptions* for Schema level DAR Creations:
        i. SDDS Database will not have Schema level Roles but it will have like DAR_SDDS_C1/C2_RO
        ii. DATAQUALITY Database will not have any Schema level roles.
    g. Database level DAR will be granted to HRDP_PD_ALL/RW/RO roles, Internally these role will be linked to developers or other users by IT Role/HRDP_DATA_QUALITY_ROLE role.
    h. Granting HRDP_DV/QA_ALL_ROLE in DV and QA, HRDP_NP_RW_ROLE in NP and HRDP_PD_RO_ROLE in PD for IT Role (Developer's Role) and "RO" in all environments for HRDP_DATA_QUALITY_ROLE.
    i. Granting required privileges to ALL, RW and RO role. For RW role we have given DELETE, UPDATE and INSERT extra from RO role privilege.
    j. Recorded Role to DAR linkage in *ROLE_DAR_MAPPING* table.
    k. Finally record the Database Name and Schema name into SCHEMA_TABLE table for reference.
3. **DGRH Role Mapping** - Configured through seed file (*infra/dbt/seeds/adm/dgrh_role_mapping_seed.csv*) which will executed through dbt
    a. Procedure Details: HRDP_ADM_PD_DB.DB_SCHEMA_SCH.DGRH_ROLE_SP()
    b. This process will grant Database Access Roles (DAR) to DGRH (End User) Roles as configured in *DGRH_ROLE_MAPPING* table.
    c. In DGRH_ROLE_MAPPING table, we are defining Long Name to Short Name relation. Ex: COMPENSATION to CMP means DGRH COMPENSATION Role will be provided with CMP and CMN schemas in HRDP_PUB_PD_DB.
4. **Custom Role Mapping** - Configured through seed file (*infra/dbt/seeds/adm/custom_role_mapping_seed.csv*) which will executed through dbt
    a. Procedure Details: HRDP_ADM_PD_DB.DB_SCHEMA_SCH.CUSTOM_ROLE_SP()
    b. This process will grant Database Access Roles (DAR) to Custom role as configured in *CUSTOM_ROLE_MAPPING* table.
    c. HRDP_DATA_QUALITY_ROLE provided with RW access for HRDP_DATAQUALITY_PD_DB and HRDP_SUPER_USER_ROLE provided with RO access for HRDP_PUB_PD_DB in all environments.
    d. Please note that configure Database name as PD Database only as procedure will convert PD to required environment when providing permission and same access level will be set for each environment.