BDH DLD -Audit & Logging Mechanism/Solution

Introduction

Purpose

The primary objective of this solution is to maintain audit metadata information in Centralized Database and to maintain Logging related information related at Zone Level in 'Zone level Database.

Proposed solution for Audit Mechanism

1. Create new DBT models using the snowflake provided metadata tables for capturing audit information and place them inside **Git Platform Repo** (**BDH_DBT_PLATFORM_REPO)**
2. The above specified/created models will be executed using DAGs and target tables for these models will be created/refreshed in **PLATFORM__AUDIT__<PREPROD/PROD> Database**.
3. DAGS will be scheduled to run in airflow as per requirements.

   Below table illustrate in which DB and the Schema, tables will be created.

Database Name	Schema Names	Tables/Views Names (linked to the Snowflake Documentation)	Comments
PLATFORM__AUDIT__<PREPROD/PROD>	**SNOWFLAKE**	GRANTS_TO_ROLES	
		WAREHOUSE_EVENTS_HISTORY	
		ACCESS_HISTORY	
		USERS	
		GRANTS_TO_USERS	
		TABLES	
		TAG_REFERENCES	
		TABLE_STORAGE_METRICS	
		QUERY_HISTORY	
		DATABASES	
		COLUMNS	
		DATABASE_STORAGE_USAGE_HISTORY	
		WAREHOUSE_METERING_HISTORY	
	FINOPS_CURATED	STORAGE_USAGE	
		WAREHOUSE_RECOMMENDER	
		OBJECT_PRIVILEGES	
		ZONEUSERROLE_MAPPING	
		BATCH_JOB_OPTIMIZATION	
		USER_ACCESS_BY_TAG	
		CREDIT_USAGE	
		QUERY_COST_RATIO Note: This custom view create on two snowflake account views. query_history warehouse_metering_history	
	FLYWAY__{env}	FLYWAY_SCHEMA_HISTORY	
	FLYWAY__{env}	FLYWAY_SCHEMA_HISTORY	
	CHANGE_LOGS__{env}		

	CHANGE_LOGS__{env}		
	FIVETRAN_LOGS		
	CORTEX	CORTEX_AISQL_USAGE_HISTORY view | Snowflake Documentation	We are not using Cortex AI Functions as part of the AI Solution, and so this table will not be populated by the solution. - Natalie Everett 19/01/2026
		CORTEX_ANALYST_USAGE_HISTORY view | Snowflake Documentation	We are not using Cortex Analyst as part of the AI Solution, and so this table will not be populated by the solution. - Natalie Everett 19/01/2026
		CORTEX_DOCUMENT_PROCESSING_USAGE_HISTORY view | Snowflake Documentation	We are not using Cortex Document AI as part of the AI Solution, and so this table will not be populated by the solution. - Natalie Everett 19/01/2026
		CORTEX_FINE_TUNING_USAGE_HISTORY view | Snowflake Documentation	We are not using Cortex Fine Tuning as part of the AI Solution, and so this table will not be populated by the solution. - Natalie Everett 19/01/2026
		CORTEX_FUNCTIONS_QUERY_USAGE_HISTORY view | Snowflake Documentation	We are not using Cortex AI Functions as part of the AI Solution, and so this table will not be populated by the solution. This view has been deprecated, CORTEX AISQL USAGE HISTORY replaced it from 17/11/2025 - Natalie Everett 19/01/2026
		CORTEX_FUNCTIONS_USAGE_HISTORY view | Snowflake Documentation	We are not using Cortex AI Functions as part of the AI Solution, and so this table will not be populated by the solution. - Natalie Everett 19/01/2026 This view has been deprecated, CORTEX AISQL USAGE HISTORY replaced it from 17/11/2025 - Natalie Everett 19/01/2026
		CORTEX_PROVISIONED_THROUGHPUT_USAGE_HISTORY view | Snowflake Documentation	We are not using Provisioned Throughput as part of the AI Solution, and so this table will not be populated by the solution. - Natalie Everett 19/01/2026
		CORTEX_SEARCH_DAILY_USAGE_HISTORY view | Snowflake Documentation	We are not using Cortex Search as part of the AI Solution, and so this table will not be populated by the solution. - Natalie Everett 19/01/2026
		CORTEX_SEARCH_REFRESH_HISTORY view | Snowflake Documentation CORTEX_SEARCH_DAILY_USAGE_HISTORY view | Snowflake Documentation	This does not seem to exist. Link is broken, and searching Snowflake Documentation cannot find any reference to this view - Natalie Everett 19/01/2026 Natalie Everett thank you for checking all of this! I see Snowflake changed the 'search refresh history' view to 'search daily usage history'. I've pasted the new link under the old one. - Tiaan de Klerk 20/01/2026
		CORTEX_SEARCH_SERVING_USAGE_HISTORY view | Snowflake Documentation	We are not using Cortex Search as part of the AI Solution, and so this table will not be populated by the solution. - Natalie Everett 19/01/2026
		CORTEX_REST_API_USAGE_HISTORY view | Snowflake Documentation	
		LOCAL schema | Snowflake Documentation	

Proposed solution for logging:

1. Design a common reusable code (EXECUTION_STATUS_LOG) macro for refreshing the final log table (EXECUTION_STATUS_LOG) and place it inside **Git Platform Repo** (**BDH_DBT_PLATFORM_REPO**)
2. Import the above developed reusable code into DPG repo (**BDH_ZONE_DBT_REPO**) along with other reusable code. This 'execution log' macro will be invoked at end of each model/snapshot/seeds/test execution, i.e. after every models execution or seeds execution or snapshots execution or test execution
3. All the tables will reside inside database **ZONE__LOGGING__DEV** database and will be used to store data for all zone.
4. Macro will be invoked using on-run-end: which is inside dbtproject.yml which required two parameters Zone.

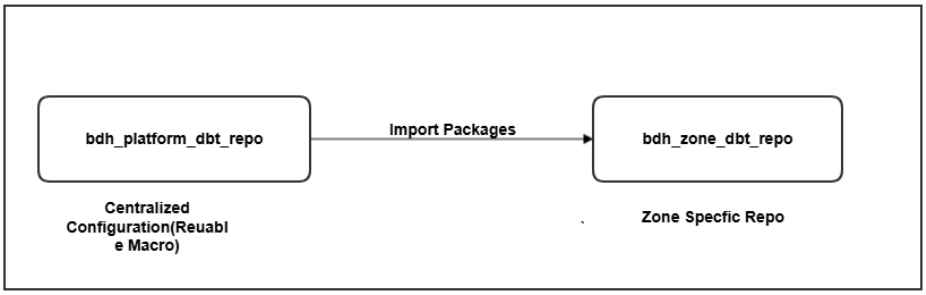
Database Name	Schema Names	Tables Names
ZONE__LOGGING__DEV	**DBT**	**MODEL_EXECUTION**
		SEED_EXCEUTION
		SNAPSHOT_EXECUTION
		TEST_EXECUTION
	CURATED	**EXECUTION_STATUS_LOG**
	RECON	**METADATA_TABLES**
		METADATA_TEST_CASES

		TEST_RESULTS

Git Repositories:

1. BDH_PLATFORM_DBT_REPO Centralized DBT Repo (Reusable components)
2. BDH_CUST_DBT_REPO ZONE Level Repo (Code at ZONE Level**)**

Design Workflow:



1. **bdh_platform_dbt_repo** git repo will hold all the **packages, reusables components**. we can import these packages into any of the repos **bdh_zone__dbt_repo** (e.g. **bdh_cust__dbt_repo**) as required.
2. **bdh_platform_dbt_repo** is a **dbt platform project repo,** which will hold common reusable macros/components (Schema, alias, db name) which will be commonly used across the platform.
3. These Audit tables models will be present in the Platform audit dbt repo and Audit tables models will populate the data in PLATFORM__AUDIT__PREPROD/PROD DB.
4. **bdh_cust__dbt_repo** is a **dbt zone project repo,** which will hold the zone specific models, dags and imported reusable macros (in form of packages) ,dbt packages from nexus repo.
5. The reusable logging macros internally refers the Seeds, Models ,Snapshot, Test Execution models present in zone project Repo. After the job's execution (Seeds/Models/Snapshot), 'Execution_status_log' macro will be also triggered in DPG project repo.
6. The Logging macros output will be populated into zone level DB (CUST__LOGGING__DEV), with tables containing attribute to identify details of Zone.

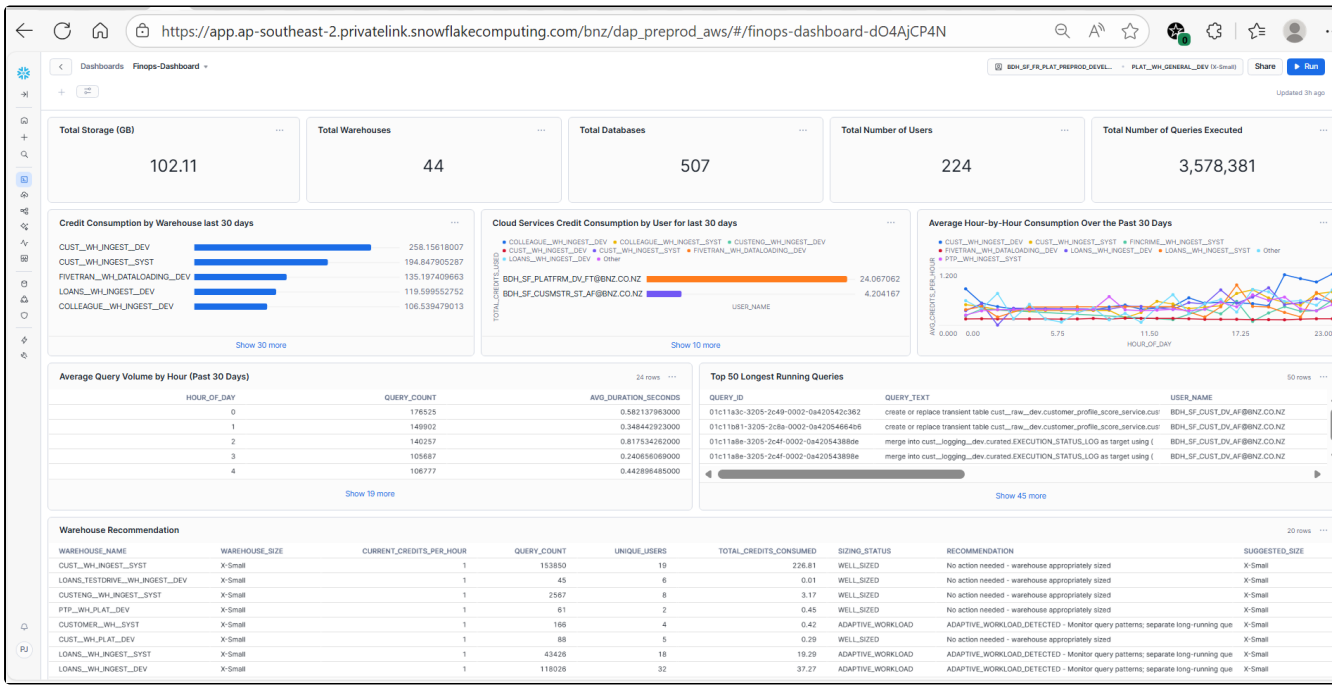
Finops Dashboard

Usage Monitoring queries are designed to identify the warehouses, queries, tools, and users that are responsible for consuming the most credits over a specified period of time.
These queries can be used to determine which of those resources are consuming more credits than anticipated and take the necessary steps to reduce their consumption.

1. Total Storage (GB)
2. Total Warehouses
3. Total Databases
4. Total Number of Users
5. Total Number of queries executed
6. Credit Consumption by Warehouse last 30 days
7. Credit Consumption by User for last 30 days
8. Average Hour by Hour consumption past 30 days
9. Average Query Volume by Hour (Past 30 Days)
10.Top 50 Longest Running Queries
11.Warehouse recommendation

Dashboard url : Finops-Dashboard - Snowflake

Note : Required AD group access the dashboard: **A_BDH_sf_fg_plat_dev_developer**



Related docs:

- Automated Reconciliation and Testing (ART) framework - Digital, Data & Analytics - BNZ Confluence