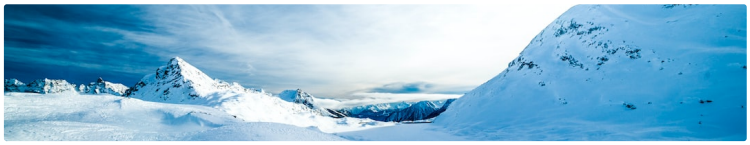


Security

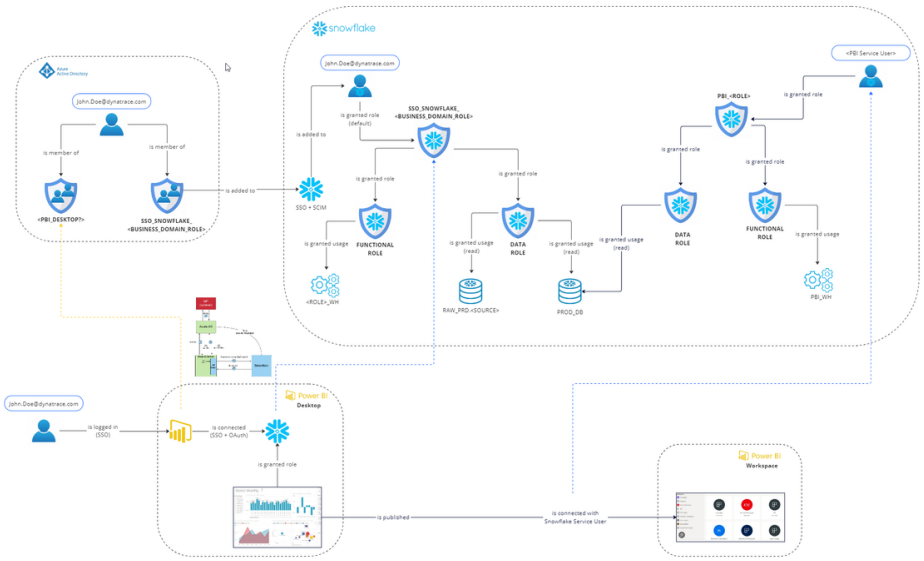
Snowflake security, particularly in the context of roles and permissions, is an essential aspect of its architecture designed to ensure data protection and access control. In Snowflake, roles are central to managing access permissions. These roles define what actions a user can perform and what objects they can access within the Snowflake environment. A user can be assigned multiple roles, each with its specific set of privileges. To streamline user management, Snowflake integrates with Active Directory (AD) groups using the System for Cross-domain Identity Management (SCIM) protocol. This integration allows for automatic synchronization of user roles and permissions between AD and Snowflake.

SSO & SCIM

The first phase of the integration between Azure AD and Snowflake is completed.

A user request access to snowflake via EDE. Upon approval by a data owner, the user is added to an AD Group. The user is automatically added to Snowflake with no data permission. A Snowflake admin will grant the appropriate functional and data roles based on the request.

During the second phase, the integration from EDE to snowflake Data and Functional roles will be fully automated.



Link to Snowflake

SCIM Configuration

Set up Snowflake custom attributes in Azure AD SCIM user provisioning

Roles and Permissions

The management of various roles and permissions in Snowflake accounts, encompassing data roles, functional roles, service roles, and Snowflake / Azure user accounts is centralized through a DBT macro hosted on GitHub.

Each Snowflake account operates independently with its unique instructions, yet all scripts adhere to a unified template and naming convention, ensuring consistency across different accounts.

Dynatrace-BusSys-BI/bs_dbt_package (github.com)