Network Strategy and Authenication

Network Strategy

Creating a network policy strategy is very important to make sure only approved users can access Snowflake from predictable and accepted IPs.

This mitigates any risks such as:

- Users logging from an undesired location
- Service Accounts are only accessible from IPs owned by them
- Employee leaves the company and still has access to credentials

WhiteList Type	Application	Dynamic /Static	User List	IPs	Process to update	Note
Account	PowerBI Server +	Dynamic	-		Posted by Microsoft on Mondays	We need to merge the POWER BI and L'Oreal Ips
Account	Snowflake Users	Semi-Static IP from L'Oreal Network			We would need to set a process to grab the IPs dynamically	We need to merge the POWER BI and L'Oreal Ips
User	DBT Cloud	Static	DBT Service Account	52.45.144.63 54.81.134.249 52.22.161.231	Posted by DBT	Contact DBT for IP information
User	GCP (Airflow, CloudRun, DataFlow…)	Static	Airflow Service Account	DEV: 34.78.5.41 QA: 104.199.93.151 PD: 34.140.115.63 NP: 34.140.251.166	Posted by GCP	
User	Breakglass policy	Open Internet		0.0.0.0		For ADMIN with MFA. We can either set it for all Admin with MFA (so all Admin can access anytime), or we can create a SP that can be run by DBT to allow the network policy to be attached to a User when run (ADMIN to access from open internet only in case of need when running a job).

Authentication

There are 4 main methods to authenticate a user into Snowflake:

- **Password**
  - We do not want any hardcoded passwords being used at the moment. Human interactions use SSO, and Process Accounts use KeyPair (with passphrase).
    In case of future need (for example a need for a connector that only allows for passwords), it is recommended to use strong password policies, https://docs.snowflake.com/en/sql-reference/sql/create-password-policy .

All users should have password UNSET (set to NULL when describe user)

- **OAUTH**
  - Power BI uses OAUTH but it has the feel of SSO on the Power BI end.
    https://docs.snowflake.com/en/user-guide/oauth-powerbi

- **KeyPair**
  - Create a Private with a Passphrase and then a Public Key.
  - The private Key and Passphrase are used in the connector (for example by DBT). It is suggested that either one encrypts them or stores them somewhere not accessible except by ADMINs.
  - The public key is used on the Snowflake User. It suggested being rotated by using the two available keys on a user: https://docs.snowflake.com/en/user-guide/key-pair-auth#configuring-key-pair-rotation
  - Security Note: Only the role-owner of the user or ADMINs (security admin or higher) has access to modify a user, and add a public key to a user. Therefore no one can alter their user to use keypair when not authorized.
- **SSO**
  - All human users will use SSO. To force that, please all users should have password UNSET (set to NULL when describe user).