01 - Snowflake-Azure SCIM Setup

Snowflake-generated SCIM tokens refresh - every 90days

1. Login to Snowflake
2. Switch to the ORGADMIN ROLE
3. Create a new account: the account should be hosted on GCP and uses the Enterprise edition
4. The account name should follow the naming convention: ***ZONE*_HRDP_*REGIONID_ENV***
    a. **ZONE:**
        i. WW: for GLOBAL or World Wide
        ii. AMER: for AMERICAS
        iii. APAC: for the APACS
        iv. EMEA: for EUROPE

    b. **HRDP:** is constant.
    c. **REGION:** It should be the REGION_ID of the chosen region at the account creation; refer to the below mapping table

REGION	REGIONID
Europe West 2 (London)	EW2
Europe West 4 (Netherlands)	EW4
US Central 1 (Iowa)	USC1
US East 4 (N. Virginia)	USE4

    d. **ENV**: DEV or PROD
5. Set an account credentials.
    a. User Name: use *FIRSTNAME_LASTNAME* pattern
    b. Password: Snowflake will ask you to change the password at first use.
    c. email: Use L'Oréal email

6. You can also do it by SQL using the below script using the role ORGADMIN:

```
      CREATE ACCOUNT "AMER_HRDP_USC1_DEV"
ADMIN_NAME='christian_elhakim_adm',
ADMIN_PASSWORD='Xxx1234567890!@#',
EMAIL='christian.elhakim@loreal.com',
EDITION=ENTERPRISE,
REGION=GCP_US_CENTRAL1,
REGION_GROUP=PUBLIC;
```

7. Get the **"Account Locator URL"**, it is the technical URL with a unique ID and should look like this: https://**du50316.us-central1**.gcp.snowflakecomputing.com. This will be used later on in order to setup the application.

8. Connect to the newly created with the previously created account; it will ask you to set a new password.

9. Execute the below SQL as ACCOUNTADMIN

```
      use role accountadmin;

create or replace role aad_provisioner;
grant create user on account to aad_provisioner;
grant create role on account to aad_provisioner;
grant role aad_provisioner to role accountadmin;
create or replace security integration aad_provisioning type=scim scim_client=azure
run_as_role='AAD_PROVISIONER';
```

10. Create a distribution list through snow using this link: https://loreal.service-now.com/myservices/?id=nr_sc_cat_item&sys_id=a8ec573ddbca30144849366af496195b
The distribution list should respect this pattern *SNOWFLAKE-HRDP-ADMINS-**ENV*** where ENV is to be selected from ***(DV,QA,NP,PD)***. The Zone The email should look like this AMER-GCP-SNOWFLAKE-HRDP-ADMINS-DV@loreal.com. The distribution list might take some time to be created.

11. Create a new Azure AD having the name of "HR DATAPLATFORM - SNOWFLAKE **ZONE** - **ENV"** using this link https://loreal.service-now.com/myservices?id=sc_cat_item&sys_id=6840560ddb5bd8504849366af496195c (you can find here an example of an already created APP https://loreal.service-now.com/nav_to.do?uri=sc_req_item.do?sys_id=3c37c41d1be8d1d8823510a38b4bcb34).

a. blocked URLSAML Sign on URL: this will be the **"Account Locator URL"** (ex: https://du50316.us-central1.gcp.snowflakecomputing.com)
b. blocked URLSAML Identifier: this will be the **"Account Locator URL"** (ex: https://du50316.us-central1.gcp.snowflakecomputing.com)
c. blocked URLSAML Reply URL: this will be the **"Account Locator URL/fed/login"** (ex: https://du50316.us-central1.gcp.snowflakecomputing.com/fed/login)
d. In the comments ask to be added to the Delegated Owners group, they will add your ADM account

12. Once the application is created (it may take some time with the support), you have to activate the provisioning, to do this follow the below steps:
    a. send an email to servicedesk-loreal@accenture.com and io.loreal.iam@accenture.com .
       "Hello
       I would like to activate the automatic provisioning for the applications (HR DATAPLATFORM - SNOWFLAKE **ZONE** - **ENV).**
       - Snowflake HRDP - PRD
       - Snowflake HRDP - Non PRD
       - HR DATAPLATFORM - SNOWFLAKE US - PRD
       - HR DATAPLATFORM - SNOWFLAKE US – DEV
       Can you please contact me in order to communicate the secret token.
       Best regards"
    b. Once contacted by the support follow the below steps:
       i. Ask the support to go on "Enterprise Applications>HR DATAPLATFORM - SNOWFLAKE **ZONE** - **ENV"** and then click on **Provisioning**
       ii. Tenant URL: this will be the **"Account Locator URL/scim/v2/"** (ex: https://du50316.us-central1.gcp.snowflakecomputing.com/scim/v2/)
       iii. Secret Token: connect to the SNOWFLAKE ACCOUNT as ACCOUNTADMIN and execute the below statement:

```
SELECT SYSTEM$GENERATE_SCIM_ACCESS_TOKEN('AAD_PROVISIONING');
```

       This will return a token that will be used for the provisioning, it looks like this: ver:1-hint:xxxx-xxxxxxxxx, share it with the support
       iv. Ask the support to go to **Users and Groups** and add the distribution list created before.
       v. Ask the support to go to the **Provisioning** and click on the button: **Start Provisioning**

13. Go to Portal.azure.com> Enterprise Applications>HR DATAPLATFORM - SNOWFLAKE **ZONE** - **ENV** and then click on **Signle sign-on**, then scroll down and download the "**Certificate (Base64)**"

14. Open the certificate using a text editor and copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- (without the begin/end)

15. Connect again to the SNOWFLAKE account using as ACCOUNT ADMIN and execute the below statement:

```
      USE ROLE ACCOUNTADMIN;
CREATE SECURITY INTEGRATION AAD_SSO
    TYPE = SAML2
    ENABLED = TRUE
    SAML2_ISSUER    = 'https://sts.windows.net/e4e1abd9-eac7-4a71-ab52-da5c998aa7ba/'
    SAML2_SSO_URL   = 'https://login.microsoftonline.com/e4e1abd9-eac7-4a71-ab52-da5c998aa7ba/saml2'
    SAML2_PROVIDER  = 'CUSTOM'
    --PAST THE BASE64 CERTIFICATE IN THE BELOW STRING
    SAML2_X509_CERT = 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX',
SAML2_SP_INITIATED_LOGIN_PAGE_LABEL = 'SSO'
SAML2_ENABLE_SP_INITIATED = TRUE;

ALTER ACCOUNT SET SSO_LOGIN_PAGE = TRUE;
```

16. Verify that the provisioning ran well:
    a. Go to the SNOWFLAKE ACCOUNT, use ACCOUNTADMIN and check the Roles in the Admin Section: you should be able to see a role with the name of the provisioned group that you have already created
    b. If the role exist, you should execute the below SQL statement by replacing "AMER-GCP-SNOWFLAKE-HRDP-ADMINS-DV" by your newly created role.

```
        USE ROLE ACCOUNTADMIN;

GRANT CREATE DATABASE ON ACCOUNT TO "AMER-GCP-SNOWFLAKE-HRDP-ADMINS-DV";
GRANT CREATE WAREHOUSE ON ACCOUNT TO "AMER-GCP-SNOWFLAKE-HRDP-ADMINS-DV";
GRANT CREATE INTEGRATION ON ACCOUNT TO "AMER-GCP-SNOWFLAKE-HRDP-ADMINS-DV";
GRANT CREATE ROLE ON ACCOUNT TO "AMER-GCP-SNOWFLAKE-HRDP-ADMINS-DV";
GRANT IMPORTED PRIVILEGES ON DATABASE SNOWFLAKE TO "AMER-GCP-SNOWFLAKE-HRDP-ADMINS-DV";
GRANT EXECUTE TASK ON ACCOUNT TO ROLE "AMER-GCP-SNOWFLAKE-HRDP-ADMINS-DV";
GRANT MANAGE ACCOUNT SUPPORT CASES on account to role "AMER-GCP-SNOWFLAKE-HRDP-ADMINS-DV";

GRANT ROLE "AMER-GCP-SNOWFLAKE-HRDP-ADMINS-DV" TO ROLE SYSADMIN;
```

17. The account is now configured to connect using SSO, you just need to add the people in the correct groups!

02 - Power Bi Integration

Setup the belon security integration in order to allow authentification through PowerBI

```
CREATE SECURITY INTEGRATION AAD_POWERBI
type = external_oauth
enabled = true
external_oauth_type = azure
external_oauth_issuer = 'https://sts.windows.net/e4e1abd9-eac7-4a71-ab52-da5c998aa7ba/'
external_oauth_jws_keys_url = 'https://login.windows.net/common/discovery/keys'
external_oauth_audience_list = ('https://analysis.windows.net/powerbi/connector/Snowflake')
external_oauth_token_user_mapping_claim = 'upn'
external_oauth_snowflake_user_mapping_attribute = 'login_name'
external_oauth_any_role_mode = 'ENABLE';
```

03 - Token Refresh

Every 6 months the token should be refreshed because it expires.

We have to setup an alert every 5 months: the previous token remains working and we can add a new token following the below procedure.

1. Ask the support to go on "Enterprise Applications>HR DATAPLATFORM - SNOWFLAKE **ZONE** - **ENV"** and then click on **Provisioning**
2. Tenant URL: this will be the **"Account Locator URL/scim/v2/"** (ex: https://du50316.us-central1.gcp.snowflakecomputing.com/scim/v2/)
3. Secret Token: connect to the SNOWFLAKE ACCOUNT as ACCOUNTADMIN and execute the below statement:

```
SELECT SYSTEM$GENERATE_SCIM_ACCESS_TOKEN('AAD_PROVISIONING');
```

   This will return a token that will be used for the provisioning, it looks like this: ver:1-hint:xxxx-xxxxxxxxx, share it with the support
4. Ask the support to go to **Users and Groups** and add the distribution list created before.
5. Ask the support to go to the **Provisioning** and click on the button: **Start Provisioning**

04 - Setup Cloud Build Account

The Cloud build account is a Key Pair authentication.

1. follow the steps within this https://docs.snowflake.com/en/user-guide/key-pair-auth.html in order to create the public and private keys (encrypted version)
2. login to the account with ACCOUNTADMIN and execute the below code while replacing the public key by the value created before

```
    CREATE OR REPLACE ROLE  "AMER-GCP-SNOWFLAKE-BUILD-NP";

GRANT CREATE DATABASE ON ACCOUNT TO "AMER-GCP-SNOWFLAKE-BUILD-NP";
GRANT CREATE WAREHOUSE ON ACCOUNT TO "AMER-GCP-SNOWFLAKE-BUILD-NP";
GRANT CREATE INTEGRATION ON ACCOUNT TO "AMER-GCP-SNOWFLAKE-BUILD-NP";
GRANT CREATE ROLE ON ACCOUNT TO "AMER-GCP-SNOWFLAKE-BUILD-NP";
GRANT IMPORTED PRIVILEGES ON DATABASE SNOWFLAKE TO "AMER-GCP-SNOWFLAKE-BUILD-NP";
GRANT EXECUTE TASK ON ACCOUNT TO ROLE "AMER-GCP-SNOWFLAKE-BUILD-NP";
GRANT EXECUTE ALERT ON ACCOUNT TO ROLE 'AMER-GCP-SNOWFLAKE-BUILD-NP';

GRANT ROLE "AMER-GCP-SNOWFLAKE-BUILD-NP" TO ROLE "AMER-GCP-SNOWFLAKE-HRDP-ADMINS-PD" ;

CREATE OR REPLACE user SA_BUILD_US_NP
password='TestPassword123!@#'
default_role = "AMER-GCP-SNOWFLAKE-BUILD-NP"
rsa_public_key='MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwPE7dLtLdk61Gzf4PAm+
qsJHiWmqdxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxx';

ALTER USER SA_BUILD_US_NP UNSET PASSWORD;

GRANT ROLE  "AMER-GCP-SNOWFLAKE-BUILD-NP"  TO USER SA_BUILD_US_NP;
```

05 - Setup ETL role

In order to mask all the data, an ETL role is created that can see all the unmasked data, but no one has access to this role.

1. create the ETL role example (this is to be done by the Zone): "AMER-GCP-SNOWFLAKE-BUILD-PD"
2. Login as ACCOUNT ADMIN to the account
3. Execute the below SQL

```
    GRANT ROLE "AMER-GCP-SNOWFLAKE-HRDP-ETL-PD" TO ROLE "AMER-GCP-SNOWFLAKE-BUILD-PD" ;
GRANT EXECUTE TASK ON ACCOUNT TO ROLE  "AMER-GCP-SNOWFLAKE-HRDP-ETL-PD" ;
```

06 - Setup alerts

In order to setup Alerts for the Zone

1. Login as ACCOUNT ADMIN to the account
2. Execute the below SQL

```
    GRANT ROLE "AMER-GCP-SNOWFLAKE-HRDP-ETL-PD" TO ROLE "AMER-GCP-SNOWFLAKE-BUILD-PD" ;
GRANT EXECUTE TASK ON ACCOUNT TO ROLE  "AMER-GCP-SNOWFLAKE-HRDP-ETL-PD" ;

GRANT EXECUTE ALERT ON ACCOUNT TO ROLE "AMER-GCP-SNOWFLAKE-HRDP-ETL-PD";

GRANT EXECUTE ALERT ON ACCOUNT TO ROLE "AMER-GCP-US_HRIS_IT_PD";
```