

GCP Infrastructure & Service Accounts details

- GCP infrastructure SA creation & accesses
 - Dev Service accounts:
 - Permissions:
 - Service-now:
 - QA Service accounts:
 - Non-Prod Service accounts:
 - Prod Service accounts:
- GCP - Snowflake Integration
 - Snowflake DEV project integration with GCS
 - Snowflake QA project integration with GCS
 - Snowflake Non-Prod project integration with GCS
 - Snowflake Prod project integration with GCS

GCP infrastructure SA creation & accesses

Dev Service accounts:

hrdp-sa-cloudbuild-dv@itg-hranalytics-gbl-ww-dv.iam.gserviceaccount.com (RITM2768459)

hrdp-sa-composer-dv@itg-hranalytics-gbl-ww-dv.iam.gserviceaccount.com (RITM2768526)

hrdp-sa-functions-dv@itg-hranalytics-gbl-ww-dv.iam.gserviceaccount.com (RITM2768597)

Permissions:

roles/editor,roles/appengine.appAdmin,roles/composer.admin,roles/dataflow.admin,roles/storage.admin,roles/iam.roleAdmin,roles/cloudbuild.builds.builder,roles/cloudbuild.serviceAgent,roles/secretmanager.secretAccessor,roles/secretmanager.secretVersionAdder,roles/cloudkms.cryptoOperator

Service-now:

https://loreal.service-now.com/myservices?id=sc_cat_item&sys_id=33dab1a6db86205048bfcd5059619bb

Requested for	JADHAV Chetan - LTI
Country	France
Project ID	itg-hranalytics-gbl-ww-dv
Zone	EMEA\SHARED
Owned by (HUB)	France
Action	Add roles
Member type	Service Account
Members	hrdp-sa-cloudbuild-dv@itg-hranalytics-gbl-ww-dv.iam.gserviceaccount.com
Roles	roles/editor,roles/appengine.appAdmin,roles/composer.admin,roles/dataflow.admin, roles/dataflow.worker, roles/storage.admin,roles/iam.roleAdmin,roles/cloudbuild.builds.builder, roles/cloudbuild.serviceAgent,roles/secretmanager.secretAccessor, roles/secretmanager.admin,roles/secretmanager.secretVersionAdder,roles/cloudkms.cryptoOperator

QA Service accounts:

hrdp-sa-cloudbuild-qa@itg-hranalytics-gbl-ww-qa.iam.gserviceaccount.com (RITM2851655)

hrdp-sa-composer-qa@itg-hranalytics-gbl-ww-qa.iam.gserviceaccount.com (RITM2850970) (RITM2985107)

hrdp-sa-functions-qa@itg-hranalytics-gbl-ww-qa.iam.gserviceaccount.com (RITM2814479)

SA	Service Account Roles
Composer Roles	roles/appengine.appAdmin,roles/composer.admin,roles/dataflow.admin, roles/dataflow.worker,roles/storage.admin,roles/iam.roleAdmin,roles/cloudbuild.builds.builder,roles/cloudbuild.serviceAgent,roles/secretmanager.secretAccessor,roles/secretmanager.secretVersionAdder,roles/cloudkms.cryptoOperator
Cloud Build Roles	roles/appengine.appAdmin,roles/cloudbuild.builds.builder,roles/cloudbuild.builds.editor, roles/composer.admin,roles/dataflow.admin,roles/storage.admin,roles/iam.roleAdmin,roles/secretmanager.secretAccessor,roles/secretmanager.secretVersionAdder, roles/secretmanager.admin,roles/cloudkms.cryptoOperator
Functions Role	roles/cloudfunctions.admin,roles/storage.admin,roles/secretmanager.secretAccessor,roles/secretmanager.secretVersionAdder,roles/cloudkms.cryptoOperator

Non-Prod Service accounts:

hrdp-sa-cloudbuild-np@itg-hranalytics-gbl-ww-np.iam.gserviceaccount.com

hrdp-sa-composer-np@itg-hranalytics-gbl-ww-np.iam.gserviceaccount.com (RITM2985268)

hrdp-sa-functions-np@itg-hranalytics-gbl-ww-np.iam.gserviceaccount.com

SA	Service Account Roles
Composer Roles	roles/appengine.appAdmin,roles/composer.admin,roles/dataflow.admin, roles/dataflow.worker,roles/storage.admin,roles/iam.roleAdmin,roles/cloudbuild.builds.builder,roles/cloudbuild.serviceAgent,roles/secretmanager.secretAccessor,roles/secretmanager.secretVersionAdder,roles/cloudkms.cryptoOperator
Cloud Build Roles	roles/appengine.appAdmin,roles/cloudbuild.builds.builder,roles/cloudbuild.builds.editor, roles/composer.admin,roles/dataflow.admin,roles/storage.admin,roles/iam.roleAdmin,roles/secretmanager.secretAccessor,roles/secretmanager.secretVersionAdder, roles/secretmanager.admin,roles/cloudkms.cryptoOperator
Functions Role	roles/cloudfunctions.admin,roles/storage.admin,roles/secretmanager.secretAccessor,roles/secretmanager.secretVersionAdder,roles/cloudkms.cryptoOperator

Prod Service accounts:

hrdp-sa-cloudbuild-pd@itg-hranalytics-gbl-ww-pd.iam.gserviceaccount.com

hrdp-sa-composer-pd@itg-hranalytics-gbl-ww-pd.iam.gserviceaccount.com (RITM2985266)

hrdp-sa-functions-pd@itg-hranalytics-gbl-ww-pd.iam.gserviceaccount.com

SA	Service Account Roles
Composer Roles	roles/appengine.appAdmin,roles/composer.admin,roles/dataflow.admin, roles/dataflow.worker,roles/storage.admin,roles/iam.roleAdmin,roles/cloudbuild.builds.builder,roles/cloudbuild.serviceAgent,roles/secretmanager.secretAccessor,roles/secretmanager.secretVersionAdder,roles/cloudkms.cryptoOperator
Cloud Build Roles	roles/appengine.appAdmin,roles/cloudbuild.builds.builder,roles/cloudbuild.builds.editor, roles/composer.admin,roles/dataflow.admin,roles/storage.admin,roles/iam.roleAdmin,roles/secretmanager.secretAccessor,roles/secretmanager.secretVersionAdder, roles/secretmanager.admin,roles/cloudkms.cryptoOperator
Functions Role	roles/cloudfunctions.admin,roles/storage.admin,roles/secretmanager.secretAccessor,roles/secretmanager.secretVersionAdder,roles/cloudkms.cryptoOperator

GCP - Snowflake Integration

Snowflake DEV project integration with GCS

1. Create GCS bucket & provide to Snowflake.
2. Create GCS bucket integration in Snowflake & provide SA to GCP team.
3. Create Custom Role in GCP with below permissions.
4. Add GCP custom role to Snowflake provided SA.

Note: Service Now request does not support Custom Roles hence the above has to be done manually. This is approved by Security team. This is implemented by CASTEX Antoine.

Integrated GCS bucket: [gcs://hrdp_data_dv/](https://gs://hrdp_data_dv/)

Service accounts: dbqwclgxuf@gcpeuropewest4-1-88d1.iam.gserviceaccount.com

Roles: Storage_Snowflake_Custome_Role

Integrated GCS bucket: [gcs://hrdp_gcs_data_eu_dv/](https://gs://hrdp_gcs_data_eu_dv/)

Service account: dbqwclgxuf@gcpeuropewest4-1-88d1.iam.gserviceaccount.com

Roles: Storage_Snowflake_Custome_Role

Snow request: (RITM2775758) (RITM2814404) (RITM2823234)

Rejected snow as Service-Now does not support custom role addition.

-

Snowflake QA project integration with GCS

Integrated GCS bucket: [gcs://hrdp_data_qa/](https://gs://hrdp_data_qa/)

Service accounts: dbqwclgxuf@gcpeuropewest4-1-88d1.iam.gserviceaccount.com

Roles: Storage_Snowflake_Custome_Role

Integrated GCS bucket: [gcs://hrdp_gcs_data_eu_qa/](https://gs://hrdp_gcs_data_eu_qa/)

Service accounts: dbqwclgxuf@gcpeuropewest4-1-88d1.iam.gserviceaccount.com

Roles: Storage_Snowflake_Custome_Role

Snowflake Non-Prod project integration with GCS

Integrated GCS bucket: [gcs://hrdp_gcs_data_eu_np/](https://gs://hrdp_gcs_data_eu_np/)

Service accounts: rxisajqgwf@gcpeuropewest4-1-88d1.iam.gserviceaccount.com

Roles: Storage_Snowflake_Custome_Role

Snowflake Prod project integration with GCS

Integrated GCS bucket: [gcs://hrdp_gcs_data_eu_pd/](https://gs://hrdp_gcs_data_eu_pd/)

Service accounts: rxisajqgwf@gcpeuropewest4-1-88d1.iam.gserviceaccount.com

Roles: Storage_Snowflake_Custome_Role

