Terraform Training Guide: GDW SFR Project

Project Context

This guide provides step-by-step instructions for working with the Terraform modules in the GDW SFR project (`gdw-sfr/`) hosted on GitHub Enterprise. It is intended for training team members on infrastructure provisioning using the predefined shared modules.

Step 1: BigQuery Dataset Creation

Location: gdw-sfr/modules/bq/

Key Files:

- locals.tf

- main.tf

How it works:

1. Define datasets in locals.tf under local.custom_dataset_names.

2. Set writer, reader, and owner mappings.

3. main.tf uses wf_bigquery-factory module.

Example Entry:
```
custom_dataset_names = {
  "my_dataset" = {
    description = "My new BQ dataset"
  }
}
dataset_writer_sa = {
  "my_dataset" = "serviceAccount:writer@project.iam.gserviceaccount.com"
}
```

Step 2: GCS Bucket Creation

Location: gdw-sfr/modules/gcs/

Key Files:

- locals.tf

- main.tf

How it works:

1. Add bucket block under local.bucket in locals.tf.

2. Define location, storage class, and IAM roles.

3. main.tf calls create_buckets module.

Example Entry:

```
bucket_name = {
  data_classification_level = "01"
  storage_class = "STANDARD"
  location = "US"
  bucket_admins = {...}
  bucket_viewers = {...}
}
```

Step 3: IAM Permissions Configuration

Location: gdw-sfr/modules/iam/locals.tf

How it works:

- Manage permissions using maps like crossproject_sa and adrolebind_sa.

Best Practices:

- Use adrolebind_sa for AD groups.

- Do not use adroleassign for binding.

Example:

```
crossproject_sa = {
  "serviceAccount:example@project.iam.gserviceaccount.com" = [
    "roles/storage.objectViewer",
```

```
  "roles/bigquery.jobUser"

 ]

}
```

Step 4: Add Labels to Pub/Sub

Location: gdw-sfr/modules/pubsub/main.tf

How it works:

- Labels are required for both topics and subscriptions.

- Pass them in the labels block of wf-pubsub-factory module.

Example:

```
labels = {

  environment = var.environment

  app_id = var.app_id

  ci_environment = var.ci_environment

  application_classification = var.application_classification

}
```

Step 5: Points to Remember

Paths to Know:

1. iam/locals.tf

2. bq/locals.tf

3. gcs/main.tf

4. gcs/locals.tf

5. composer/locals.tf

IAM Tips:

- Check Console > IAM > Limit grantable roles.

- Raise a ticket to IAM Ops if not listed (SLA 2-3 weeks).

Labeling Rules:

Terraform Training Guide: GDW SFR Project

- Always add:

  - Pub/Sub labels

  - Topic labels

- Never assign TokenCreator role to AD groups.

Approval:

- CDM team merges into main branch after review.

Final Notes

- Follow naming conventions strictly.

- Keep shared module versions consistent.

- Check IAM and labeling before changes.

This document is intended as a live training reference.