# CDMP – Five9 Event-Driven File Transfer via STS (No Admin Roles)

## 1. Overview

This document outlines an event-driven architecture between Five9 and CDMP projects using Google Cloud Platform's Storage Transfer Service (STS) for recurring file transfers. It eliminates the need for admin roles and uses fine-grained IAM permissions with Terraform to orchestrate infrastructure and service integration.

## 2. Components Involved

- Five9 GCS Bucket (Source)  
- CDMP GCS Bucket (Destination)  
- Cloud Function (in CDMP)  
- Pub/Sub Topics & Subscriptions (One for trigger, one for STS completion)  
- Cloud Composer (CDMP environment) for DAG execution  
- STS Jobs (Dynamically created and deleted)  
- Terraform for infrastructure provisioning and IAM bindings

## 3. Workflow

1. Five9 uploads files into its GCS bucket.  
2. Object Finalize event triggers a Pub/Sub topic (configured on Five9 bucket).  
3. The Pub/Sub sends message to CDMP-hosted Cloud Function.  
4. Cloud Function triggers Airflow DAG in CDMP Composer.  
5. DAG dynamically creates STS job to pull from Five9 to CDMP.  
6. The STS job uses completion notification Pub/Sub topic.  
7. DAG listens to this topic to proceed once STS is complete.  
8. Based on initial message flag, DAG optionally deletes source files and deletes the STS job.

## 4. IAM Permissions

✅ Permissions on Five9 Side:

- Service account used by STS:  
 • roles/storage.objectViewer on Five9 bucket  
 • roles/pubsub.publisher on STS completion topic (CDMP side)  
  
- Cloud Function service account (CDMP):  
 • roles/pubsub.subscriber on trigger topic

✅ Permissions on CDMP Side:

- STS service account:  
 • roles/storage.objectAdmin on CDMP bucket  
  
- Cloud Composer service account:  
 • roles/composer.user  
 • roles/storage.objectViewer (on source)  
 • roles/storage.objectAdmin (on destination)  
 • roles/storagetransfer.user  
  
- Cloud Function service account:  
 • roles/composer.worker (to trigger DAG via REST API)

## 5. Expected Pub/Sub Message from Five9

{  
 "bucket": "five9-upload-bucket",  
 "name": "folder1/file123.csv",  
 "project\_id": "five9-project-id",  
 "delete\_after\_transfer": true  
}

## 6. Terraform IAM Notes

- Use IAM binding modules for each service account.  
- Avoid usage of roles like `roles/storagetransfer.admin`.  
- Grant minimal required permissions as noted above.  
- Cloud Function should be provisioned with environment variables like:  
 COMPOSER\_ENV, COMPOSER\_LOCATION, PROJECT\_ID.

## 7. Architecture Diagram

Refer to the attached architecture diagram below for visual representation:

