Cross-Org GCS Transfers via STS + Composer with VPC-SC

This guide outlines how to securely configure VPC Service Controls (VPC-SC) for GCS-to-GCS transfers between:

- Org1 / Project A / Bucket: five9
- Org2 / Project B / Bucket: cdmp

Transfers are triggered by Composer DAGs using Storage Transfer Service (STS) in push and pull modes.

VPC-SC Setup: five9 to cdmp (Push & Pull)

Use Case:

- Push: Org1/Project A/Composer triggers STS to transfer files from five9 (source) to cdmp (destination)
- Pull: Org2/Project B/Composer triggers STS to pull from five9 to cdmp

Required Setup for Both Directions:

1. Enable Required APIs:
   - storage.googleapis.com (GCS)
   - storagetransfer.googleapis.com (STS)

2. Add All Involved Projects into a Common VPC-SC Perimeter:
   - Project A (Composer, Source Bucket: five9)
   - Project B (Destination Bucket: cdmp)

3. Add Services to the VPC-SC Perimeter:
   - storage.googleapis.com
   - storagetransfer.googleapis.com

4. IAM Setup:
   - Composer SA in push project (e.g. Project A) needs:
     - storagetransfer.admin
     - storage.objectViewer on five9
     - storage.objectCreator on cdmp
   - STS Service Account:
     - roles/storage.objectViewer on five9
     - roles/storage.objectCreator on cdmp

5. If Projects Are in Different Perimeters:
   - Use Access Levels (allow SA identity)
   - Configure Egress Policies between orgs/projects

6. STS Job Type:

- Use pre-created STS job
- Trigger using Composer DAG via `transferJobs().run(...)`
- Use prefix filtering (`includePrefixes`) and timestamp filtering via DAG

Diagram: Single-Direction STS Workflow

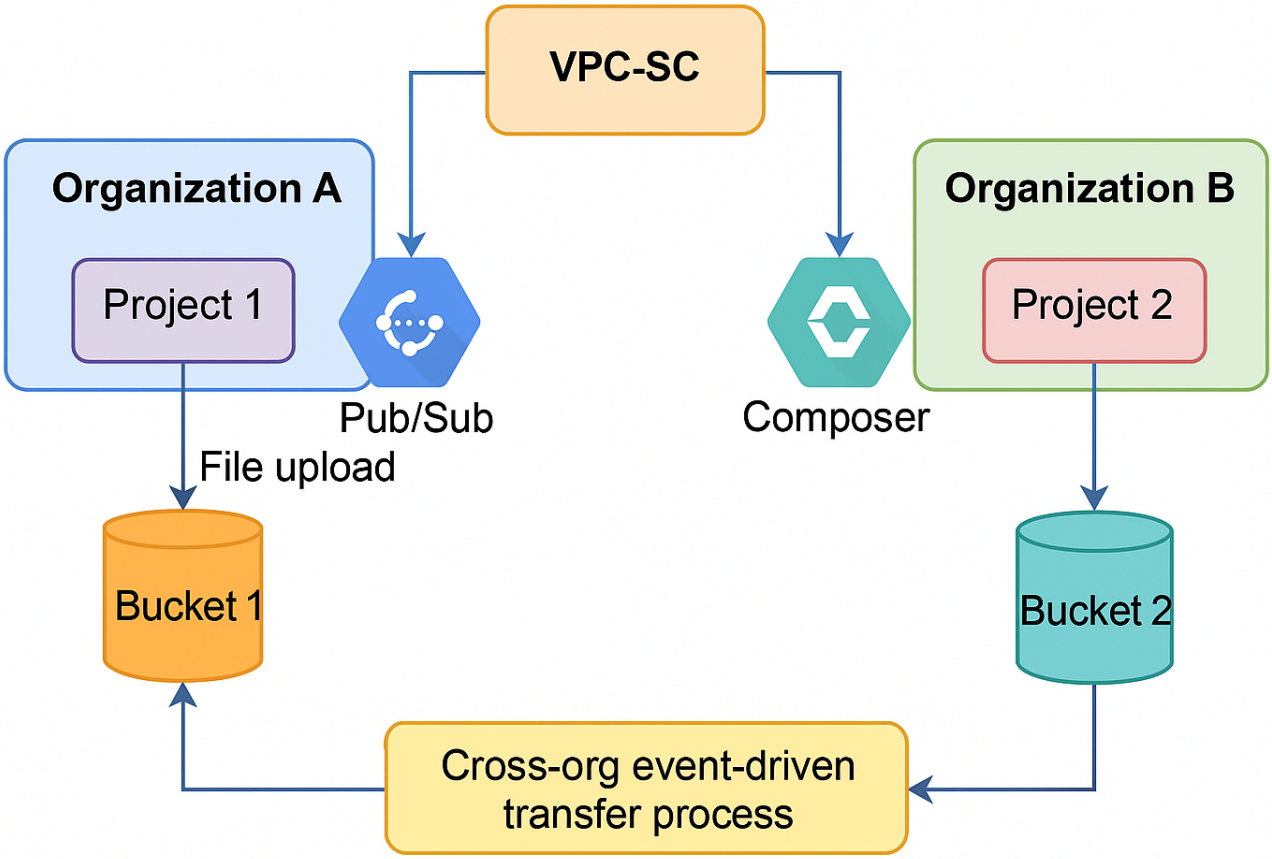

Diagram: Push & Pull STS Workflow (five9 <-> cdmp)