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

Org-Level IAM Role Assignments for Cross-Org STS

To enable secure and functional push and pull transfers between Org1 and Org2 using Storage Transfer Service (STS) and Cloud Composer, each organization must grant specific IAM roles to service accounts or AD group identities from the other organization.

Org1 Responsibilities (Source: five9 | Composer Location):

---

1. Grant the following roles on Bucket five9 (source):
   - To: STS SA or Composer SA from Org2 (if pull)
   - Role: roles/storage.objectViewer

2. Grant the following project-level roles in Project A (Composer):
   - To: Composer SA in Project A
   - Role: roles/storagetransfer.admin

3. Optional: If using an AD group, assign the AD group access to required buckets/services.

Org2 Responsibilities (Destination: cdmp):

---

1. Grant the following roles on Bucket cdmp (destination):
   - To: STS SA or Composer SA from Org1 (if push)
   - Role: roles/storage.objectCreator

2. If Composer runs in Org2 for pull jobs:
   - Grant roles/storagetransfer.admin in Project B (cdmp) to Composer SA

Cross Identity Mapping:

- For Push (Org1 triggers):
  - Org1 needs access to write to Org2's bucket cdmp
  - Org2 must authorize Org1's SA with roles/storage.objectCreator on cdmp

- For Pull (Org2 triggers):
  - Org2 needs read access to Org1's bucket five9
  - Org1 must authorize Org2's SA with roles/storage.objectViewer on five9

Recommendations:

- Use AD group identities or named service accounts
- Always follow least-privilege principle
- Validate permissions by testing STS manually

VPC-SC Ingress and Egress Rules (Detailed)

When using separate VPC-SC perimeters for Org1 and Org2, STS job execution must be explicitly allowed via ingress and egress policies.

Ingress Policy (for Pull: Org2 pulling from Org1):

- Perimeter Target: Project A (Org1, five9 bucket)
- Direction: INGRESS
- Identity Type: Service Account (Composer SA or STS SA from Org2)
- Access Level: Create Access Level including allowed identities
- Allowed Services:
  - storage.googleapis.com
  - storagetransfer.googleapis.com

Egress Policy (for Push: Org1 pushing to Org2):

- Perimeter Target: Project B (Org2, cdmp bucket)
- Direction: EGRESS
- Destination: All Projects or specific Project B
- Identity Type: Service Account (Composer SA or STS SA in Org1)
- Services:
  - storage.googleapis.com
  - storagetransfer.googleapis.com
- Recommended Condition:
  - Source: Project A
  - Identity in Access Level: true
- Enable `use_restrictions` and test using dry-run before enforcing

Best Practice:

- Monitor Cloud Audit Logs for denied VPC-SC events (policyDenied)
- Avoid wildcard-based access; use fine-grained access levels

- Work with Org Policy Admins to get cross-org access policies reviewed

Diagram: Single-Direction STS Workflow

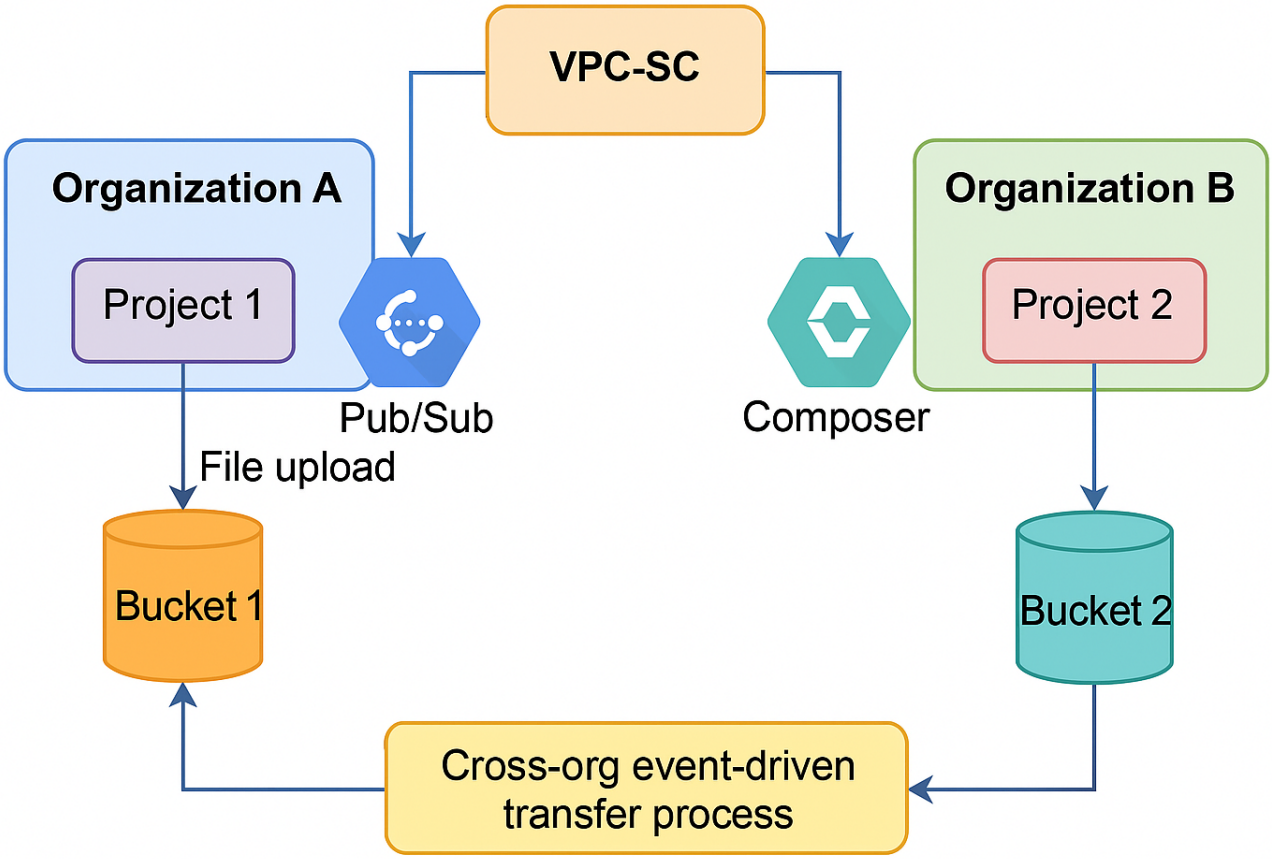

Diagram: Push & Pull STS Workflow (five9 <-> cdmp)