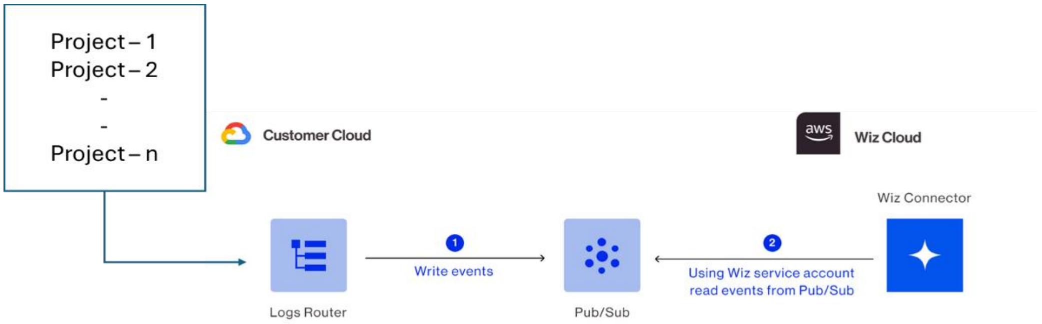
Table of Contents

1. Document Overview

This document includes detail steps on integrating wiz.io to GCP at Organizational level and connection to GCP cloud events. Connect Wiz to Google Cloud Platform (GCP) environment to enable Wiz to collect data about cloud environment and provide insights.

Overview: Wiz uses several techniques to scan your entire cloud environment without a single agent or sidecar deployed on your workloads. This assures that you can get Wiz up and running across your environment in minutes without suffering from the coverage gaps that the limited deployment of agents typically causes.

Reference Architecture:



2. Wiz.io integration to GCP

2.1: Required roles

To deploy on the Organization-level, the user performing the connection must have sufficient permissions, either as a GCP owner, or a user with these org-level roles:

- roles/iam.serviceAccountAdmin
- roles/iam.organizationRoleAdmin
- roles/iam.securityAdmin

2.2: Connect to GCP:

2.2.1: Start creating connector in Wiz as per below documentation.
Connect to GCP

Wiz.io admin can do the first step by choosing.

- Cloud provider as **GCP** and GCP organization ID.
- For installation type select **Standard**.
- And for Connector scope select **Organization**, Folder or Project.
- In the Deploy section, enter the required **Organization**, Folder, and Project IDs depending on the Connector scope previously selected.
- As a next step select a script, upon running which will create wiz roles in our GCP.

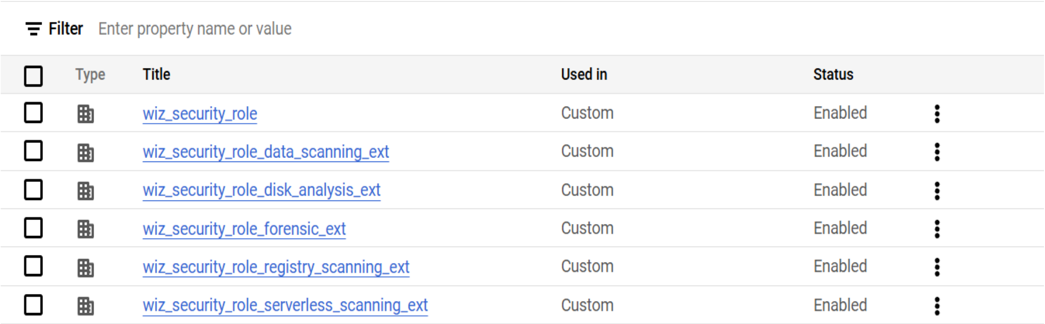
Example script is provided below.

2.2.2: Create Wiz roles in GCP (One-time activity)

- Run the below script in cloud shell. It will create Wiz roles in our GCP.

```
curl -fsSL https://wizio-public.s3.amazonaws.com/deployment-v2/gcp/cli/wiz-gcp.sh | bash /dev/stdin managed-standard organization-deployment --organization-id=302491745572 --wiz-managed-id=wiz3b092d76d84233639af50370c21@prod-us1-300113.iam.gserviceaccount.com --with-serverless-scanning --with-data-scanning --with-forensic
```

- Validate the wiz roles created as part of above step in GCP at Org level.



□	Type	Title	Used in	Status	
□	▦	wiz_security_role	Custom	Enabled	⋮
□	▦	wiz_security_role_data_scanning_ext	Custom	Enabled	⋮
□	▦	wiz_security_role_disk_analysis_ext	Custom	Enabled	⋮
□	▦	wiz_security_role_forensic_ext	Custom	Enabled	⋮
□	▦	wiz_security_role_registry_scanning_ext	Custom	Enabled	⋮
□	▦	wiz_security_role_serverless_scanning_ext	Custom	Enabled	⋮

2.2.3: Finish creating the connector in Wiz

Once wiz.io roles are created and validated, need to select project scope (select default – all projects) this will be done by Wiz.io admin.

2.3: Connect to GCP cloud events:

Below is the documentation on how to connect to GCP Cloud events.

Connect to GCP Cloud Events

2.3.1: Configure GCP Audit logs to stream to pubsub topic

- Organization level
- We have configured the GCP connector at Organization level and setting up the cloud events at the Organization level as well.

Terraform script: (one-time activity)

```
provider "google" {}

module "wiz_cloud_events" {
  source                = "https://downloads.wiz.io/customer-files/gcp/wiz-gcp-cloud-events-terraform-module.zip"
  integration_type      = "ORGANIZATION"
  org_id                = "302491745572"
  project_id            = "prj-shrd-mntr-4"
  service_account_email = "wiz3b092d76d84233639af50370c21@prod-us1-300113.iam.gserviceaccount.com"

  enable_wiz_defend_log_sources = "true"
}

output "wiz_cloud_events_configuration" {
  value = module.wiz_cloud_events
}
```

This module will create a pubsub topic and subscription_id in provided centralized project. Which will be used in next step to connect to wiz.

Topic: wiz-export-audit-logs

Subscription ID: wiz-export-audit-logs-sub

2.3.2: Connect Wiz to the new pubsub

- User who has access to Wiz (Settings->Deployments) as per the documentation.
- For the GCP Connector responsible for the environment where you are enabling cloud events integration and event-triggered scanning, click More Options > Edit.
- Select Enable Cloud Events Integration.
- For Deployment Method, select Manual.
- Enter details of Topic and Subscription_ID, the pubsub topic and subscription_id created in previous step and save.

2.3.3: Validate GKE audit logs and Streaming GCP data event to wiz. These will be streaming as we set (enable_wiz_defend_log_sources) to TRUE in terraform script as we have Wiz Defend License.

3. Metadata

GCP Organization	: questdiagnostics.com
Organization id	: 302491745572
GCP project	: prj-shrd-mntr-4
Pubsub topic	: projects/prj-shrd-mntr-4/topics/wiz-export-audit-logs
Subscription ID	: wiz-export-audit-logs-sub
Service account	: wiz3b092d76d84233639af50370c21@prod-us1-300113.iam.gserviceaccount.com
roles	: roles/wiz_security_role roles/wiz_security_role_data_scanning_ext roles/wiz_security_role_disk_analysis_ext roles/wiz_security_role_forensic_ext roles/wiz_security_role_registry_scanning_ext roles/wiz_security_role_serverless_scanning_ext