

Introduction to Google Cloud for AWS professionals

Irek Pastusiak

CorkSec August 2024

GCP services

AWS	Google Cloud
EC2	Compute Engine
EKS	Google Kubernetes Engine
Lambda	Cloud Functions
RDS	Cloud SQL
S3	Cloud Storage
Shield, WAF	Cloud Armor
...	...



IAM – GCP overview – 1/5

- Users
 - Cloud Identity (admin.google.com): AUTHN
 - IAM (console.cloud.google.com): AUTHZ
- Service accounts
 - IAM

IAM – AWS IAM policy – 2/5

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "rds:*",
      "Resource": ["arn:aws:rds:region:*:*"]
    },
    {
      "Effect": "Allow",
      "Action": ["rds:Describe*"],
      "Resource": ["*"]
    }
  ]
}
```

IAM – GCP IAM roles – 3/5

 Artifact Registry Service Agent  EDIT ROLE

ID	roles/artifactregistry.serviceAgent
Role launch stage	General Availability

Description

Gives the Artifact Registry service account access to managed resources.

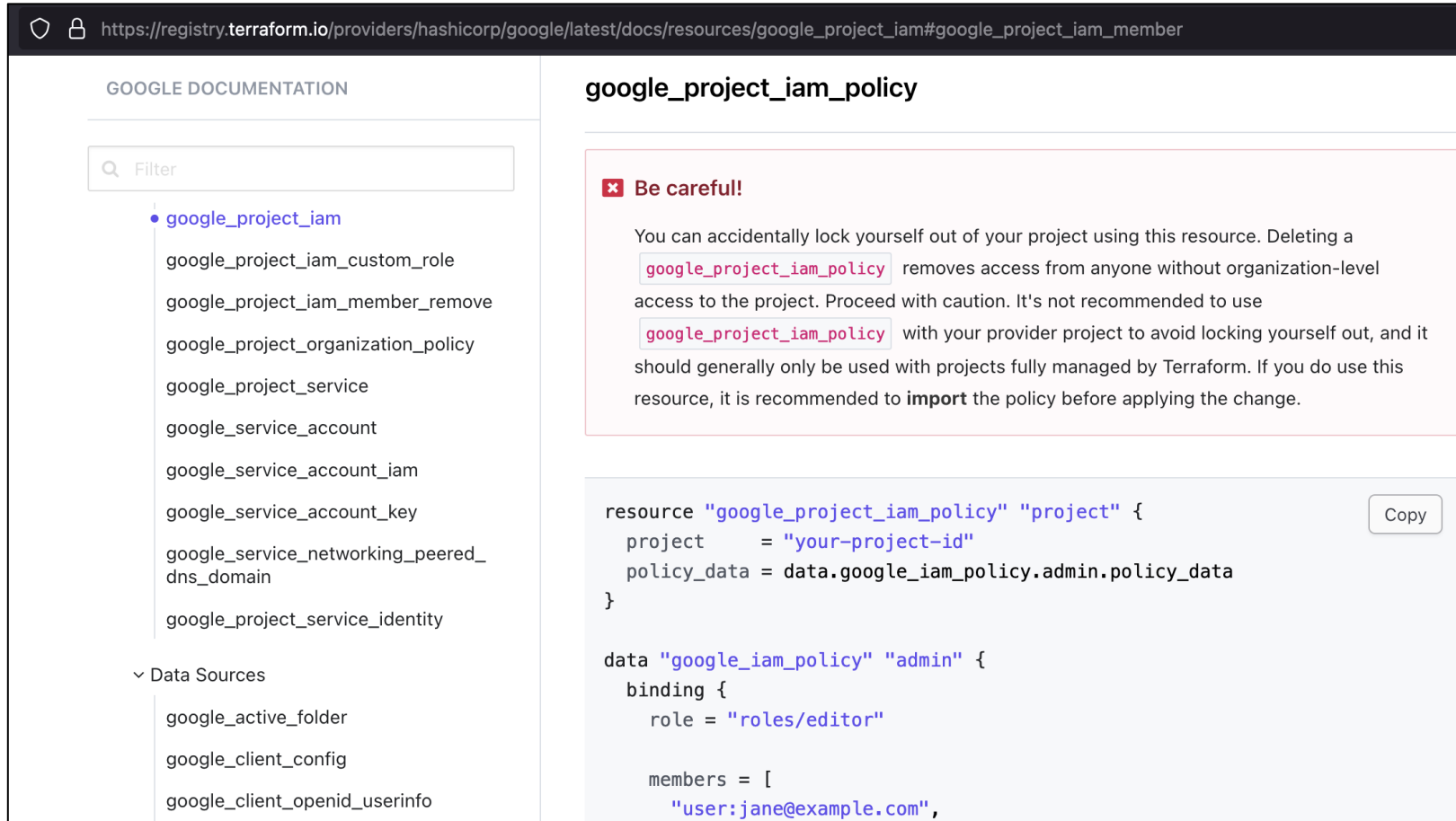
5 assigned permissions

- artifactregistry.repositories.downloadArtifacts
- artifactregistry.repositories.get
- artifactregistry.repositories.readViaVirtualRepository
- artifactregistry.versions.delete
- pubsub.topics.publish

IAM – GCP project IAM policy – 4/5

```
bindings:
  - members:
      - serviceAccount:sds-gke-worker@<project_id>.iam.gserviceaccount.com
    role: roles/artifactregistry.reader
  - members:
      - serviceAccount:service-<project_number>@gcp-sa-artifactregistry.iam.gserviceaccount.com
    role: roles/artifactregistry.serviceAgent
  - members:
      - serviceAccount:sds-gke-worker@<project_id>.iam.gserviceaccount.com
    role: roles/autoscaling.metricsWriter
  - members:
      - serviceAccount:<project_number>@cloudbuild.gserviceaccount.com
      - serviceAccount:cloud-builder-db@<project_id>.iam.gserviceaccount.com
      - serviceAccount:cloud-builder@<project_id>.iam.gserviceaccount.com
    role: roles/cloudbuild.builds.builder
  - ...
etag: BwYRQRqgUH0=
version: 3
```

IAM – GCP Terraform provider – 5/5



The screenshot shows the Terraform Registry page for the `google_project_iam_policy` resource. The left sidebar contains a search bar and a list of resources under the `google_project_iam` category. The main content area displays the resource name, a warning box, and a code snippet for creating the resource.

GOOGLE DOCUMENTATION

Filter

- `google_project_iam`
 - `google_project_iam_custom_role`
 - `google_project_iam_member_remove`
 - `google_project_organization_policy`
 - `google_project_service`
 - `google_service_account`
 - `google_service_account_iam`
 - `google_service_account_key`
 - `google_service_networking_peered_dns_domain`
 - `google_project_service_identity`
- ▼ Data Sources
 - `google_active_folder`
 - `google_client_config`
 - `google_client_openid_userinfo`

google_project_iam_policy

⚠ Be careful!

You can accidentally lock yourself out of your project using this resource. Deleting a `google_project_iam_policy` removes access from anyone without organization-level access to the project. Proceed with caution. It's not recommended to use `google_project_iam_policy` with your provider project to avoid locking yourself out, and it should generally only be used with projects fully managed by Terraform. If you do use this resource, it is recommended to **import** the policy before applying the change.

```
resource "google_project_iam_policy" "project" {
  project      = "your-project-id"
  policy_data = data.google_iam_policy.admin.policy_data
}
```


Copy

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}
```

https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/google_project_iam#google_project_iam_member

GCP API focus – 1/2



Secret Manager API

[Google Enterprise API](#)

Stores sensitive data such as API keys, passwords, and certificates. Provides convenience while...

[ENABLE](#) [TRY THIS API](#)

[OVERVIEW](#) [PRICING](#) [DOCUMENTATION](#) [RELATED PRODUCTS](#)

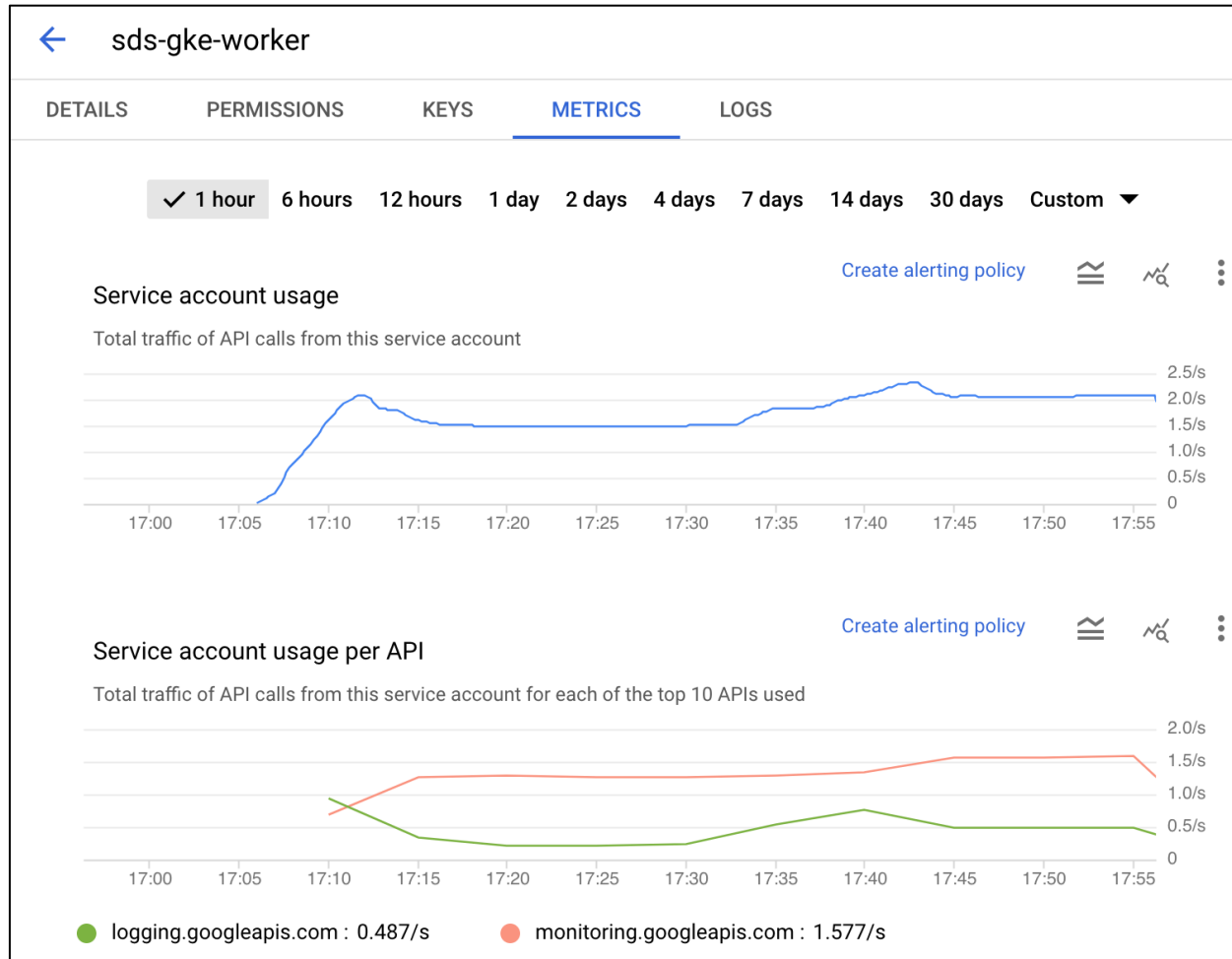
Overview

Stores sensitive data such as API keys, passwords, and certificates. Provides convenience while improving security.

Additional details

Type: [SaaS & APIs](#)
Last product update: 22/07/2022
Category: [Google Enterprise APIs](#)
Service name: secretmanager.googleapis.com

GCP API focus – 2/2



<https://console.cloud.google.com>

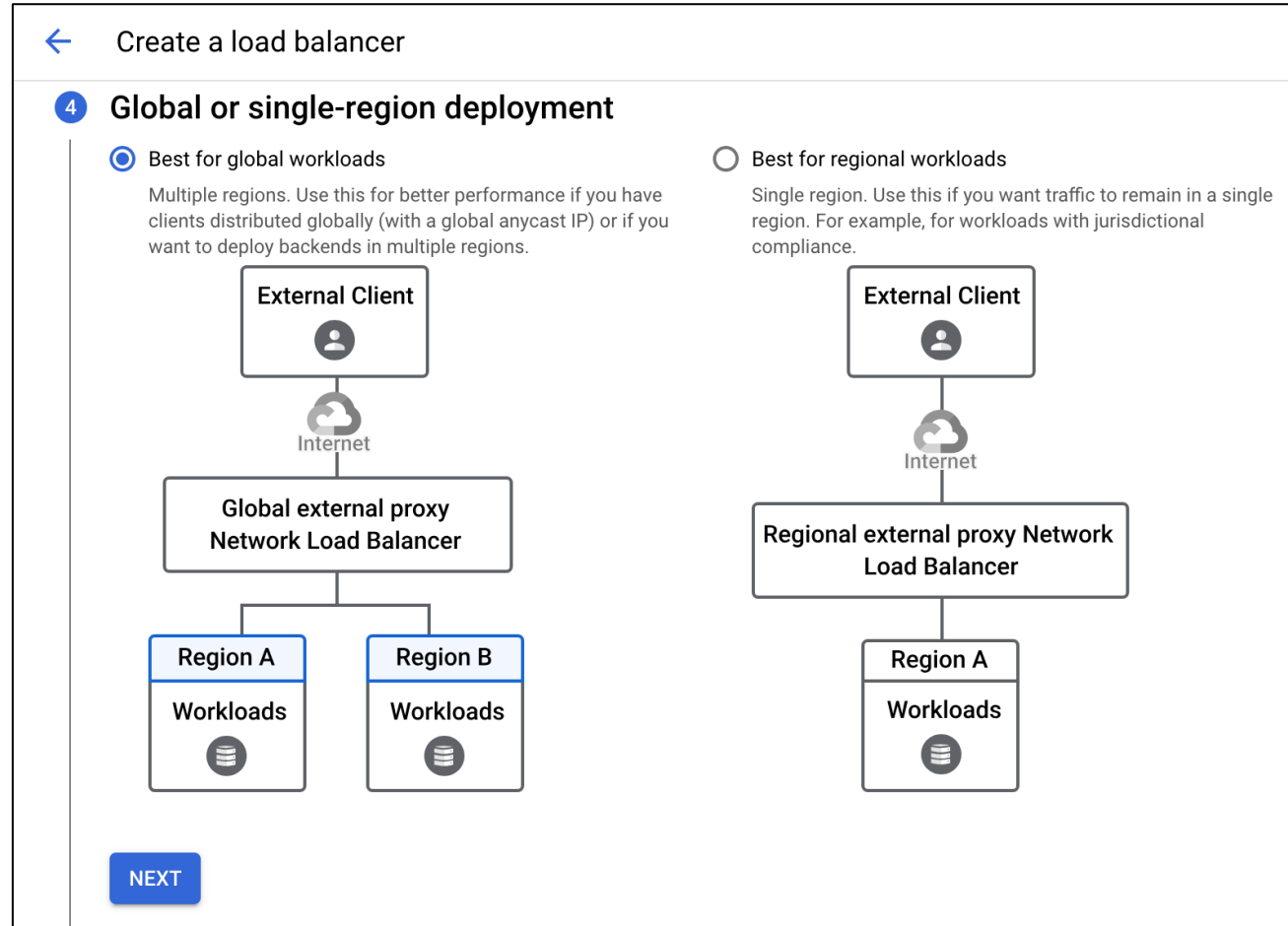
GCP global focus – resource view – 1/6

VM instances						
<div><div>CREATE INSTANCE</div><div>IMPORT VM</div><div>REFRESH</div><div>LEARN</div></div>						
<div>INSTANCESOBSERVABILITYINSTANCE SCHEDULES</div>						
VM instances						
<div><div>Filter</div><div>Enter property name or value</div><div>?</div><div>III</div></div>						
<input type="checkbox"/>	Status	Name ↑	Zone	Recommendations	In use by	Connect
<input type="checkbox"/>	✓	demo-instance-mumbai	asia-south1-a			SSH ▾ ⋮
<input type="checkbox"/>	✓	demo-instance-us	us-central1-a			SSH ▾ ⋮
<input type="checkbox"/>	✓	gke-sds-cluster-sds-node-pool-9bda23ed-kd7w	europa-west3-c		gke-sds-cluster-sds-no	SSH ▾ ⋮
<input type="checkbox"/>	✓	gke-sds-cluster-sds-node-pool-f13e52b8-0hs8	europa-west3-b		gke-sds-cluster-sds-no	SSH ▾ ⋮

GCP global focus – networking – 2/6

AWS	Google Cloud
VPC is regional	VPC is global
Subnet is zonal	Subnet is regional

GCP global focus – load balancing – 3/6



GCP global focus – multi-region – 4/6

Products available by location				
Deploy resources in specific zones, regions and multi-regions.				
	AMERICAS	EUROPE	ASIA PACIFIC	MIDDLE EAST
				AFRICA
				MULTI-REGION
Products	Americas	Europe	Asia Pacific	
Anthos	us	emea	apac	
Artifact Registry	us	europa	asia	
BigQuery ^{2,5}	us	europa		
Cloud Storage ^{2,5}	us nam4	europa eur4	asia asia1	
	nam3 nam6 nam7 nam8			

<https://cloud.google.com/about/locations#multi-region>

GCP global focus – zones – 5/6

! 27 Apr 2023 06:39 PDT

Summary: Multiple Google Cloud services in the europe-west9-a zone are impacted

Description: Water intrusion in a data center in europe-west9 caused a multi-cluster failure that led to a shutdown of multiple zones. Impact is now limited to services in europe-west9-a. There is no ETA for full recovery of operations in europe-west9-a at this time. We expected to see extended outages for some services. Customers are advised to failover to other zones/regions if they are impacted.

The following services have fully recovered in europe-west9: Google Cloud Storage (GCS) Cloud Key Management Service (KMS) Cloud Identity and Access Management (IAM).

The following services have recovered in europe-west9-b and europe-west9-c, but continue to be impacted in europe-west9-a: Google Compute Engine (GCE) Cloud Run Google Cloud Load Balancer (GCLB) DataProc Cloud SQL

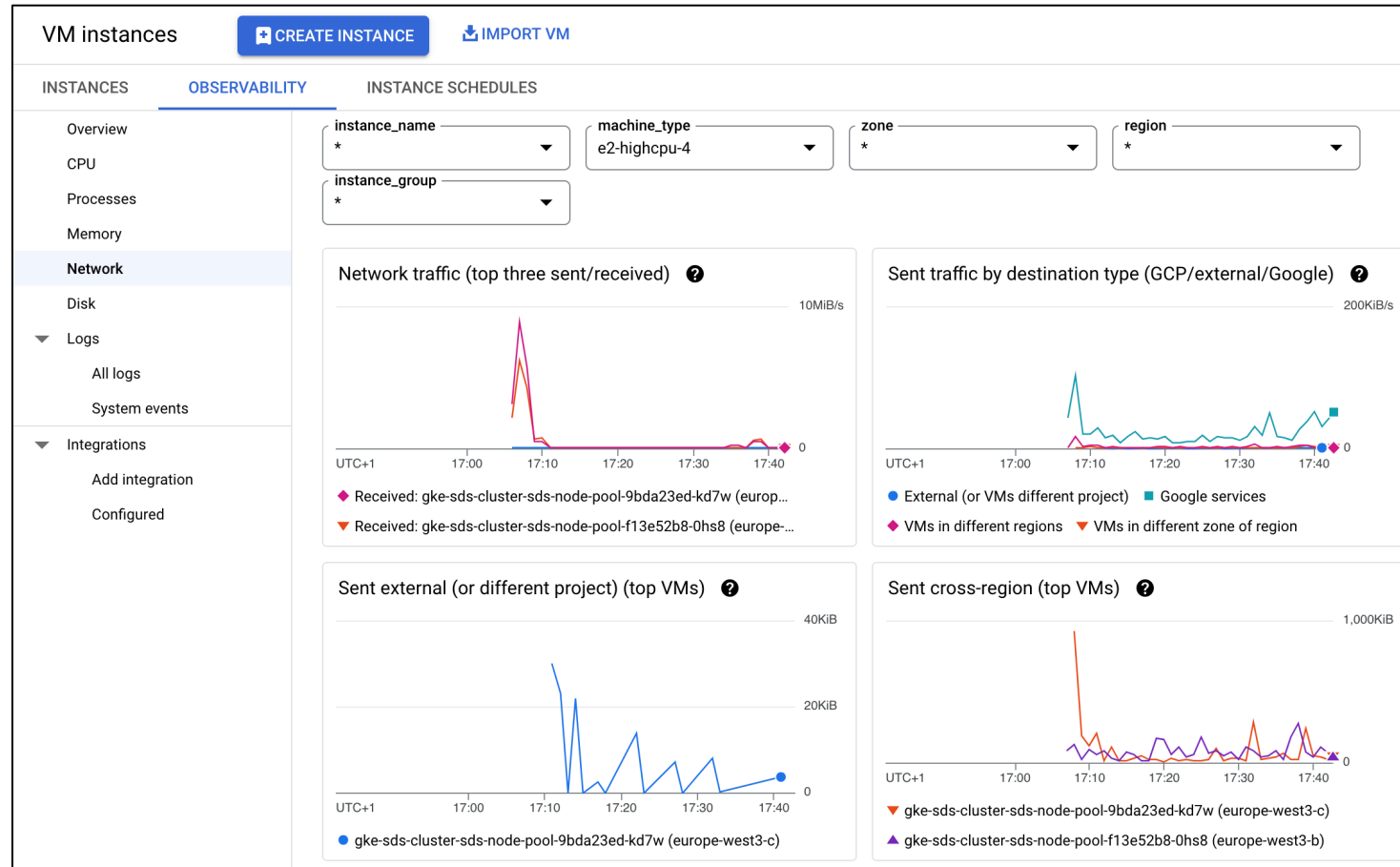
We will provide an update by Thursday, 2023-04-27 11:00 US/Pacific, or upon any significant development.

Diagnosis: Customers may be unable to access Cloud resources in europe-west9 region.

Workaround: Customers can failover to zones in other regions.

To protect against the loss of an entire region due to natural disaster, have a disaster recovery plan and know how to bring up your application in the unlikely event that your primary region is lost. See [application deployment considerations](#) for more information.

GCP global focus – metrics – 6/6



GCP network security – firewall rules – 1/2

Logs

Turning on firewall logs can generate a large number of logs, which can increase costs in Logging.[Learn more](#)

☒ On
☐ Off

▼ **SHOW LOGS DETAILS**

Network *
sds-vpc ▼ ?

Priority *
1000 [COMPARE](#) ?

Priority can be 0–65535

Direction of traffic ?
☒ Ingress
☐ Egress

Action on match ?
☒ Allow
☐ Deny

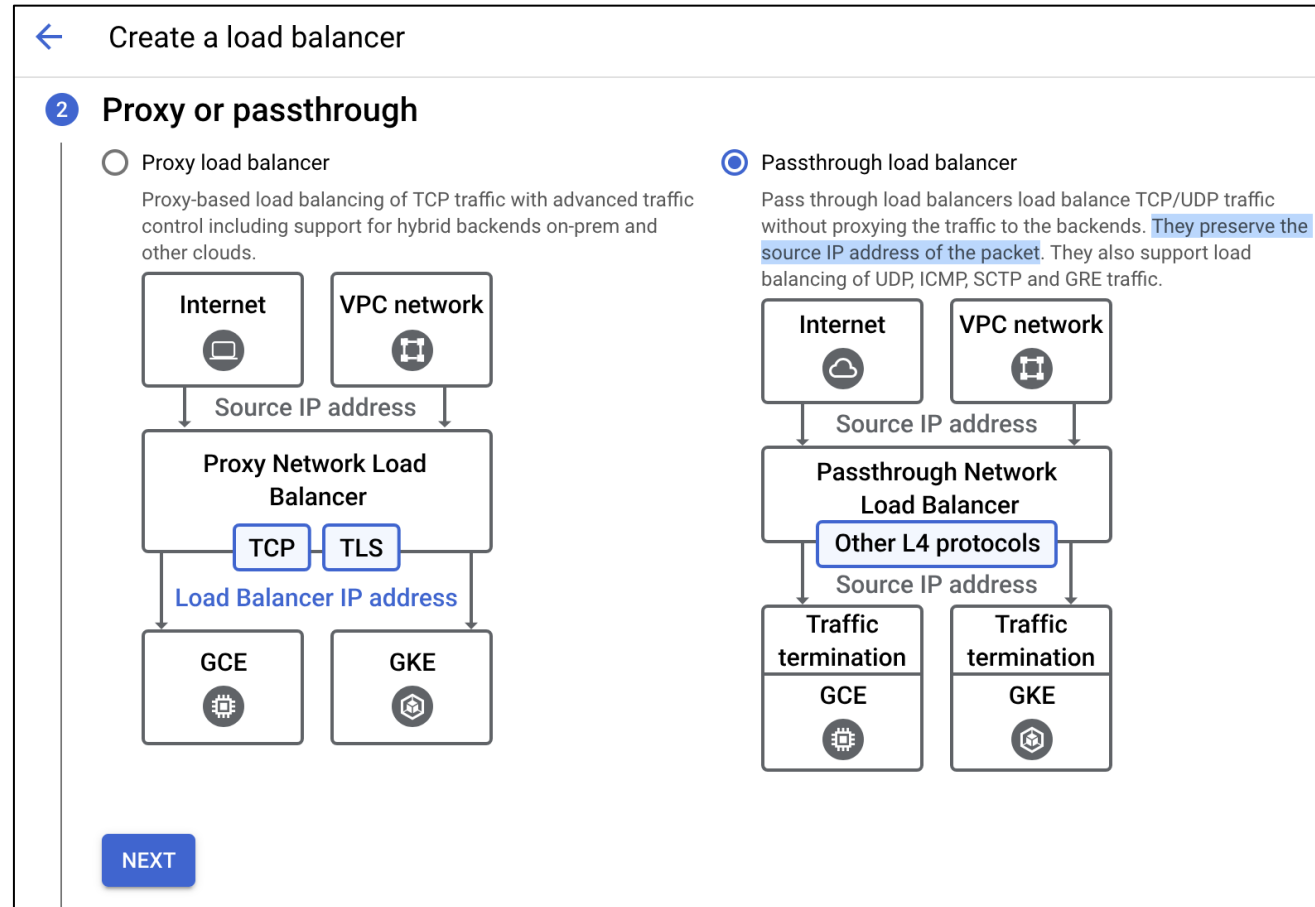
Targets ?

All instances in the network

Specified target tags

Specified service account

GCP network security – load balancing – 2/2



The End

Questions