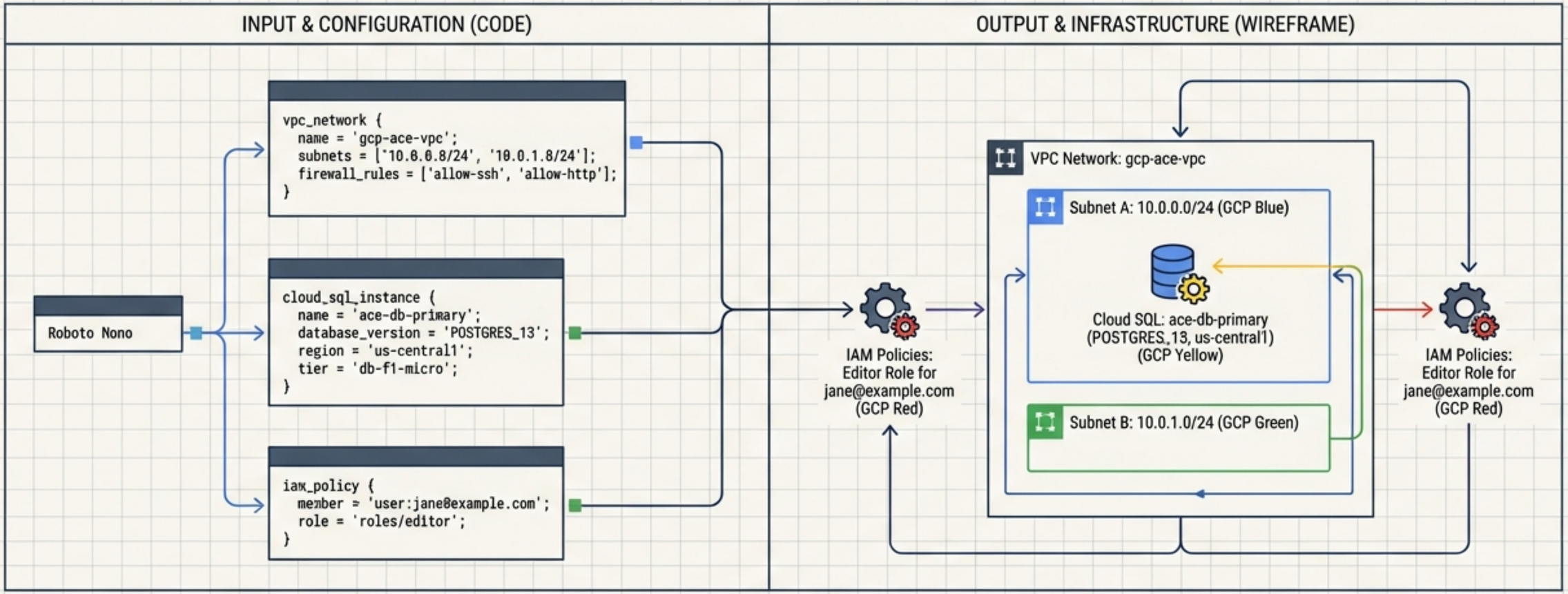
Laying the Cloud Foundation

ACE Certification Preparation Guide: Section 1

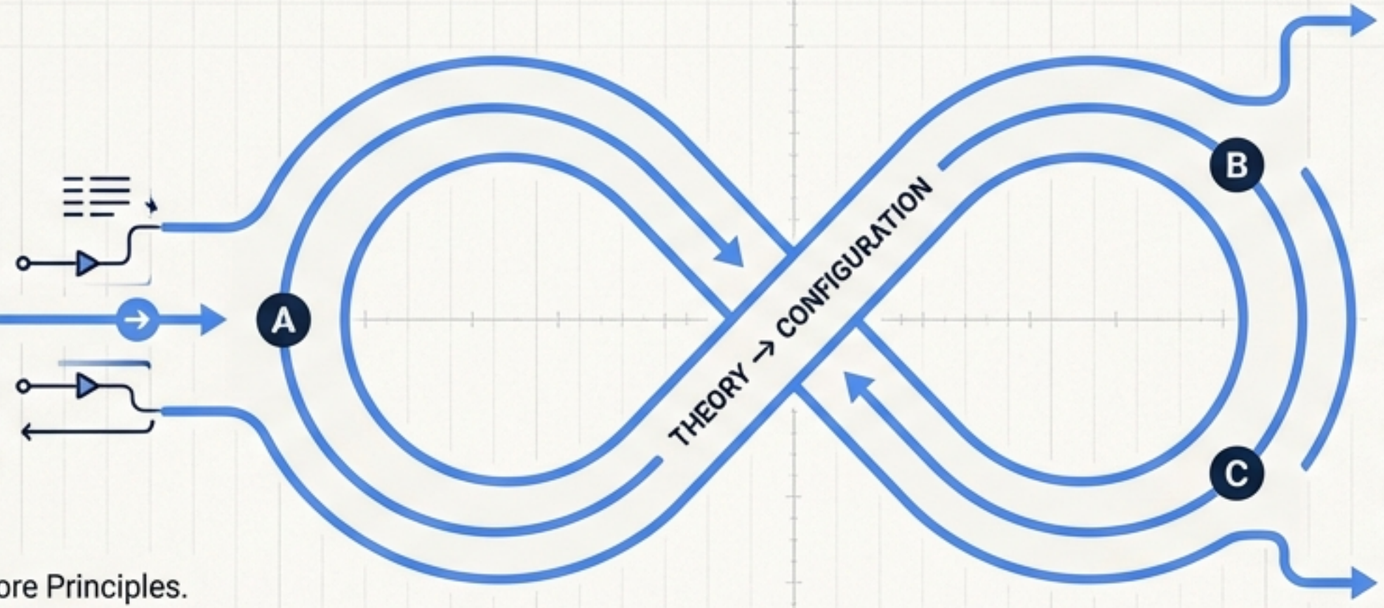


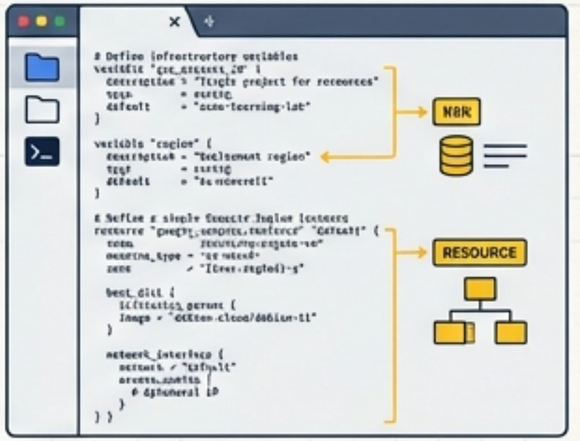

```
Target:  GCP Associate Cloud Engineer (ACE)
Vehicle: Tech Equity RAD Platform
Status:  Blueprint Ready
```

The Concept-to-Console Learning Engine

The Concept

ACE Exam Theory & Core Principles.





The Input: RAD UI

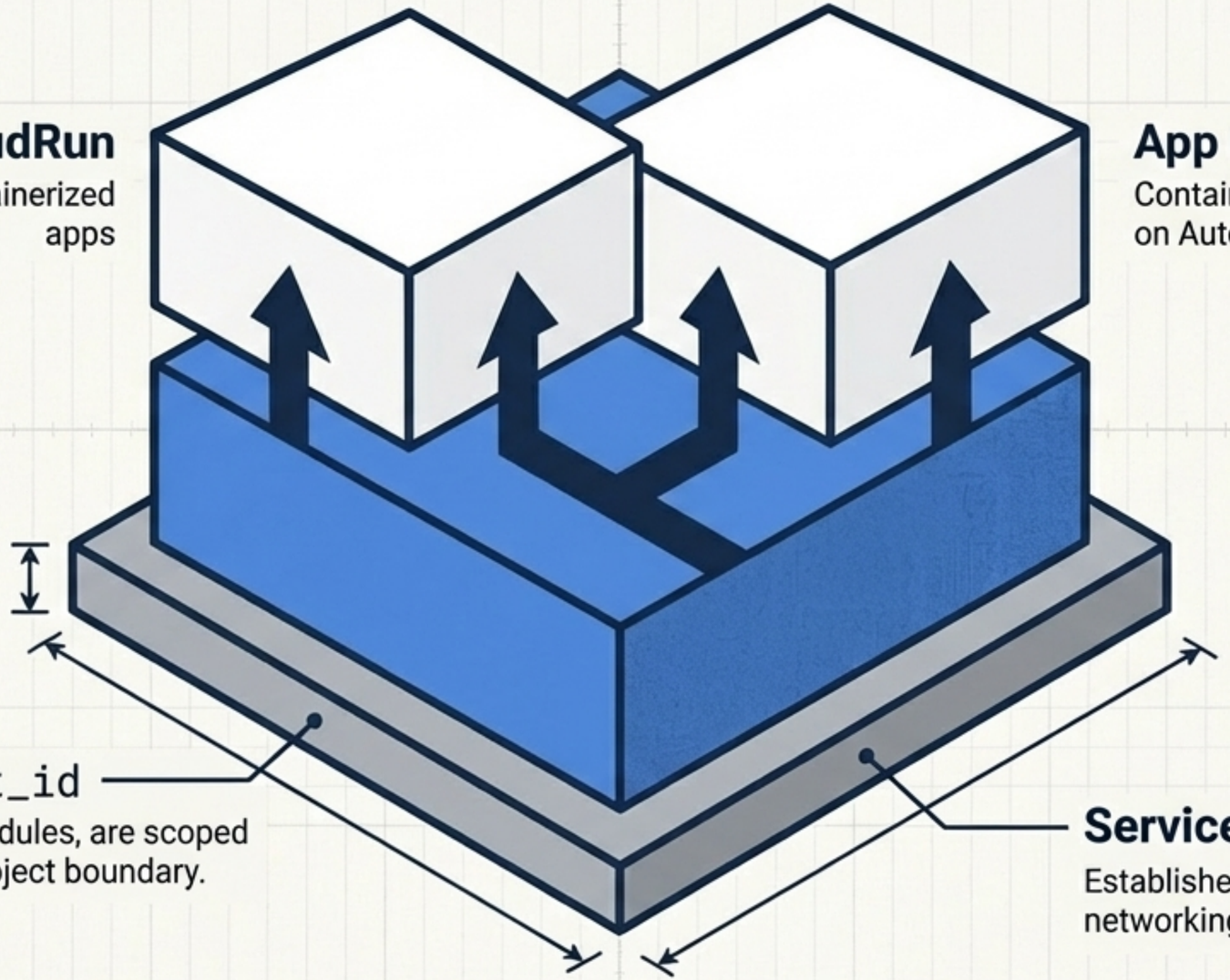
Configure variables to codify infrastructure.

The Output: GCP Console

Verify deployed resources and metrics.

> Mastery requires closing the loop. Every configuration maps to a verifiable outcome.

The Foundational Layer Cake



App CloudRun

Serverless containerized apps

App GKE

Containerized workloads on Autopilot

`existing_project_id`

All resources, across all modules, are scoped to this single immutable project boundary.

Services GCP

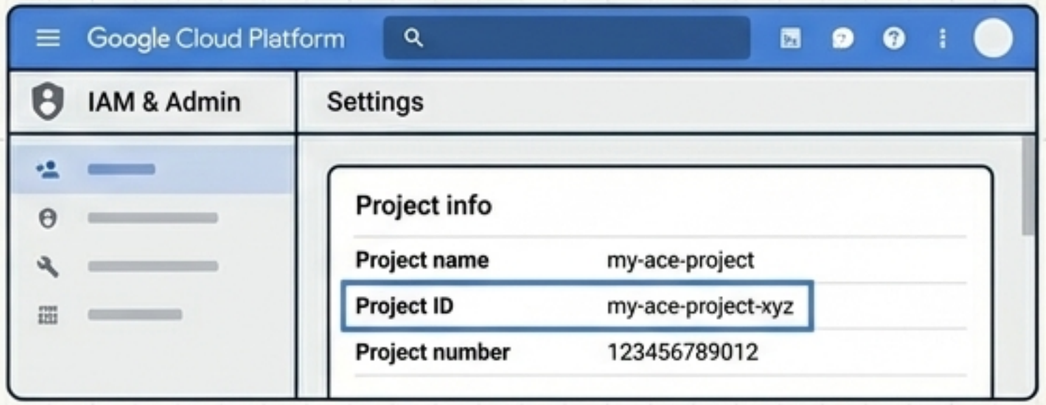
Establishes shared infrastructure: VPC networking, databases, IAM, APIs.

Mapping the Resource Hierarchy

RAD UI Pane (Input)

```
existing_project_id = "my-ace-project-xyz"
```

Console Pane (Output)



The 3 Critical Identifiers

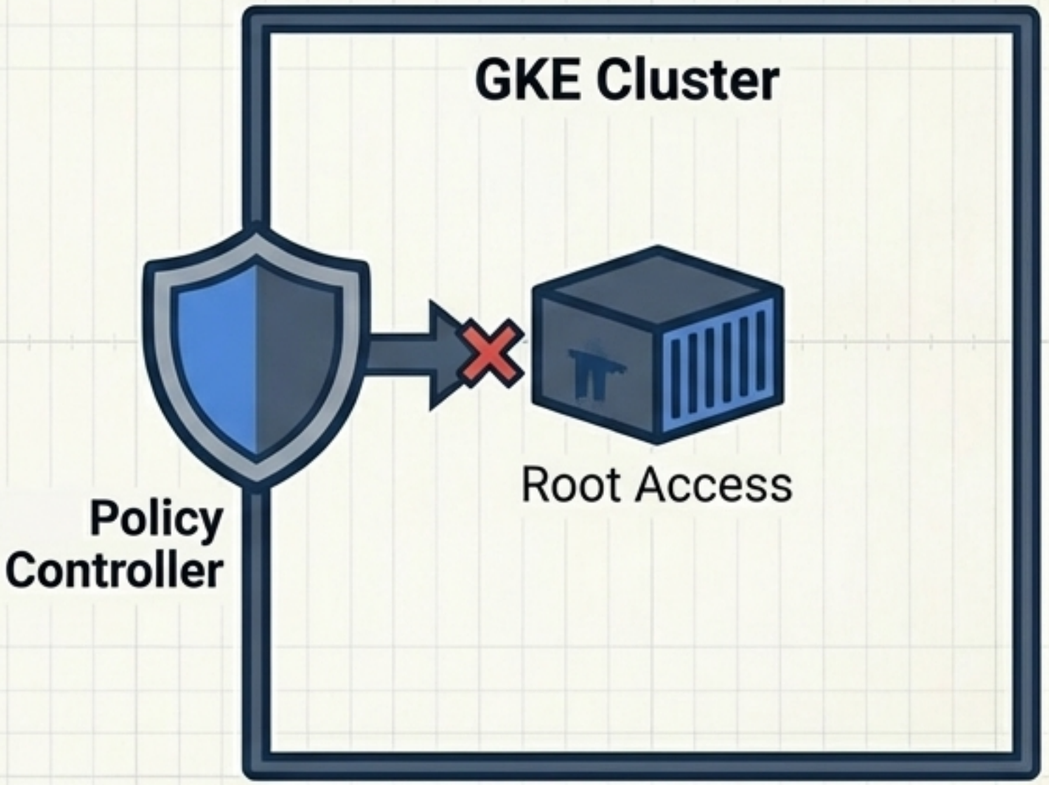
1. **Project ID**: Immutable, globally unique, set at creation. (ACE Exam focus)
2. **Project Number:** Auto-generated, immutable integer.
3. **Project Name:** User-defined, mutable display name.

Guardrails at Scale: Organizational Policies

enable_vpc_sc

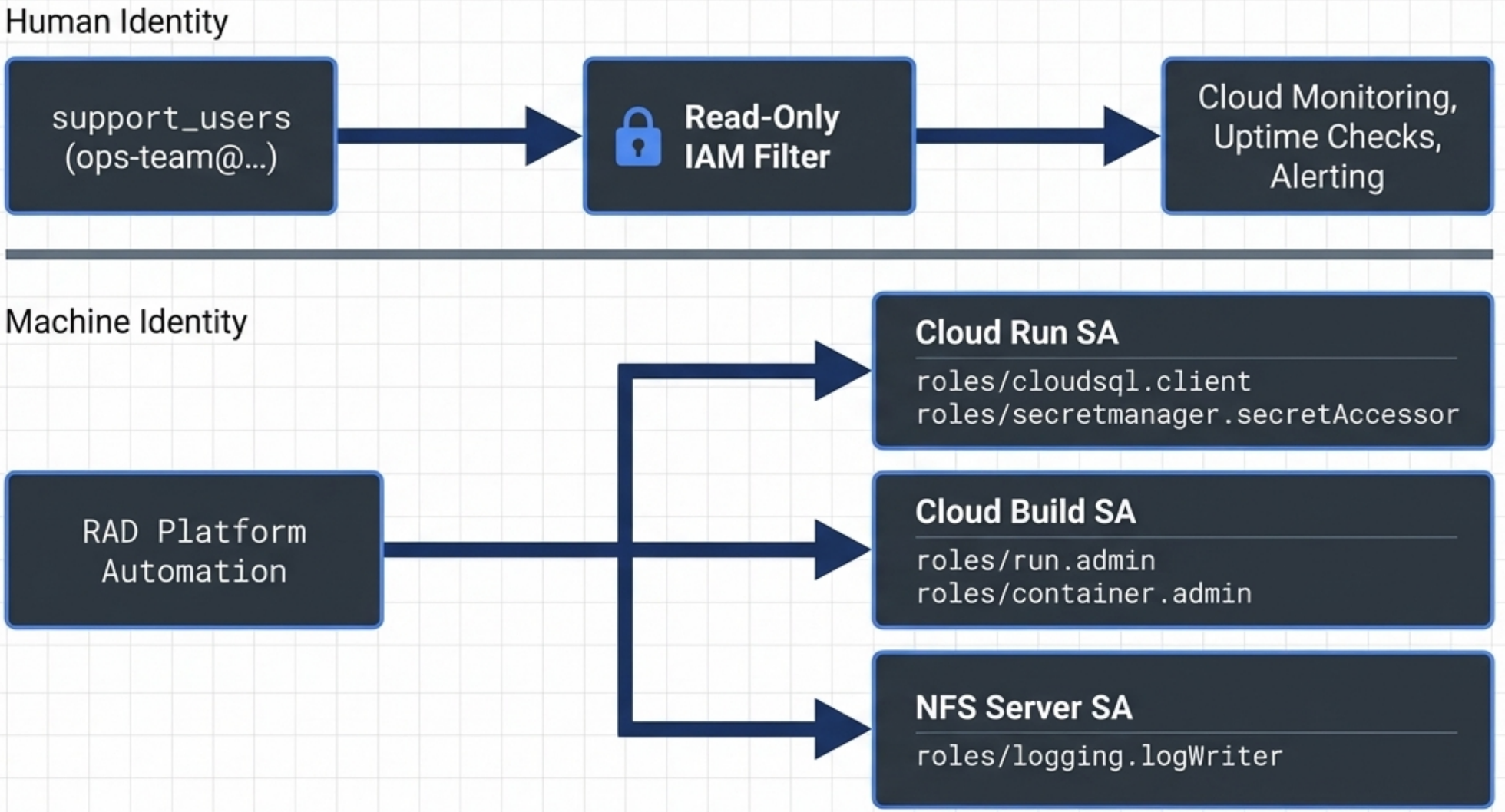
VPC Service Perimeter blocks data exfiltration by restricting API access to internal network traffic.

configure_policy_controller



Kubernetes admission control rejects non-compliant workloads before they start.

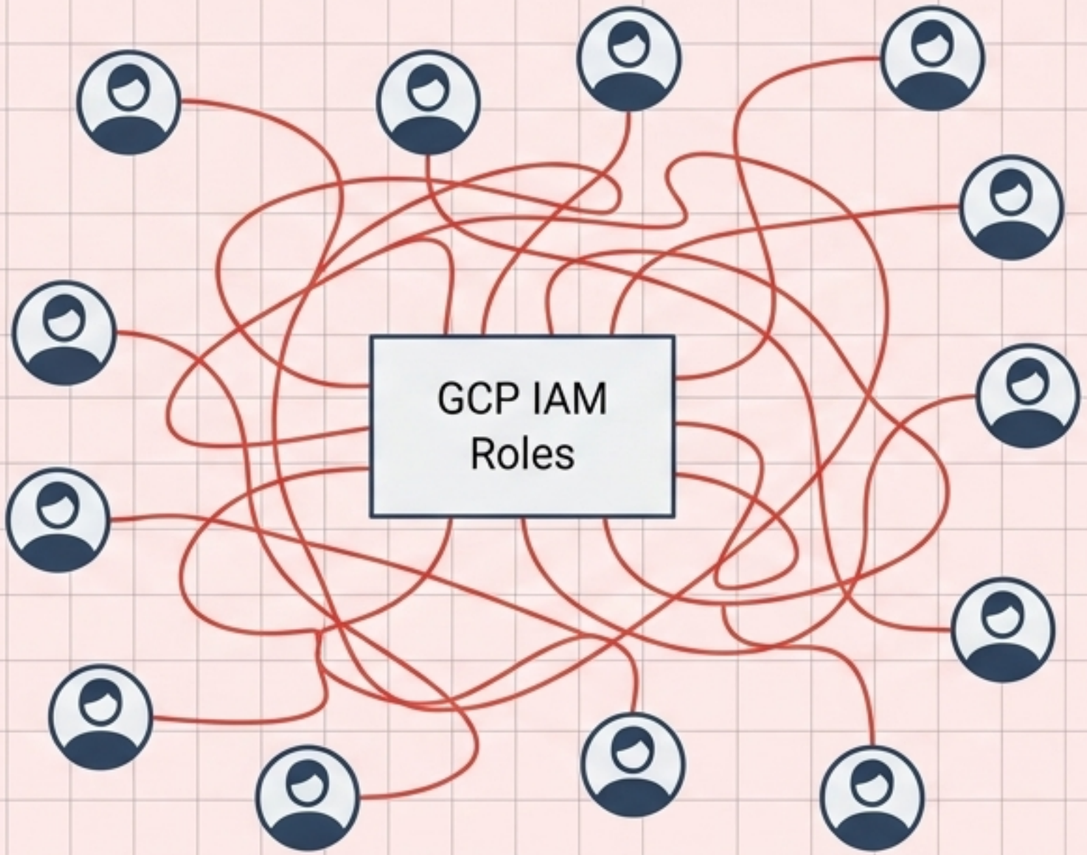
IAM: Human vs. Machine Identities



Automated Human Identity Management

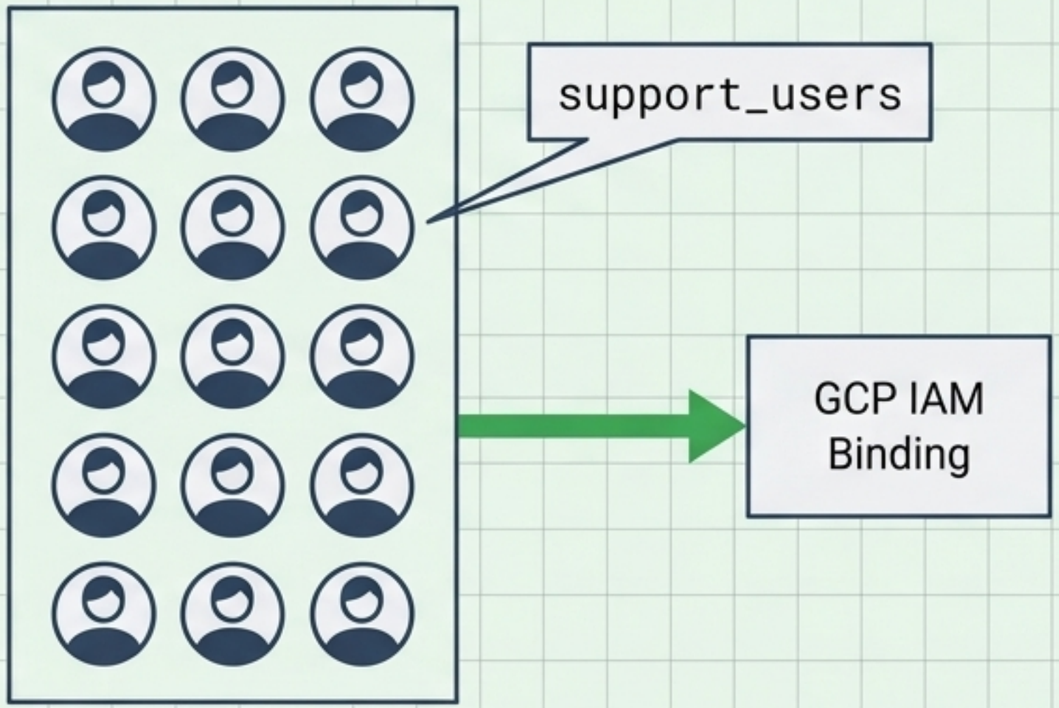
Google Cloud

Anti-Pattern



High maintenance, security risk upon offboarding.

ACE Exam Pattern

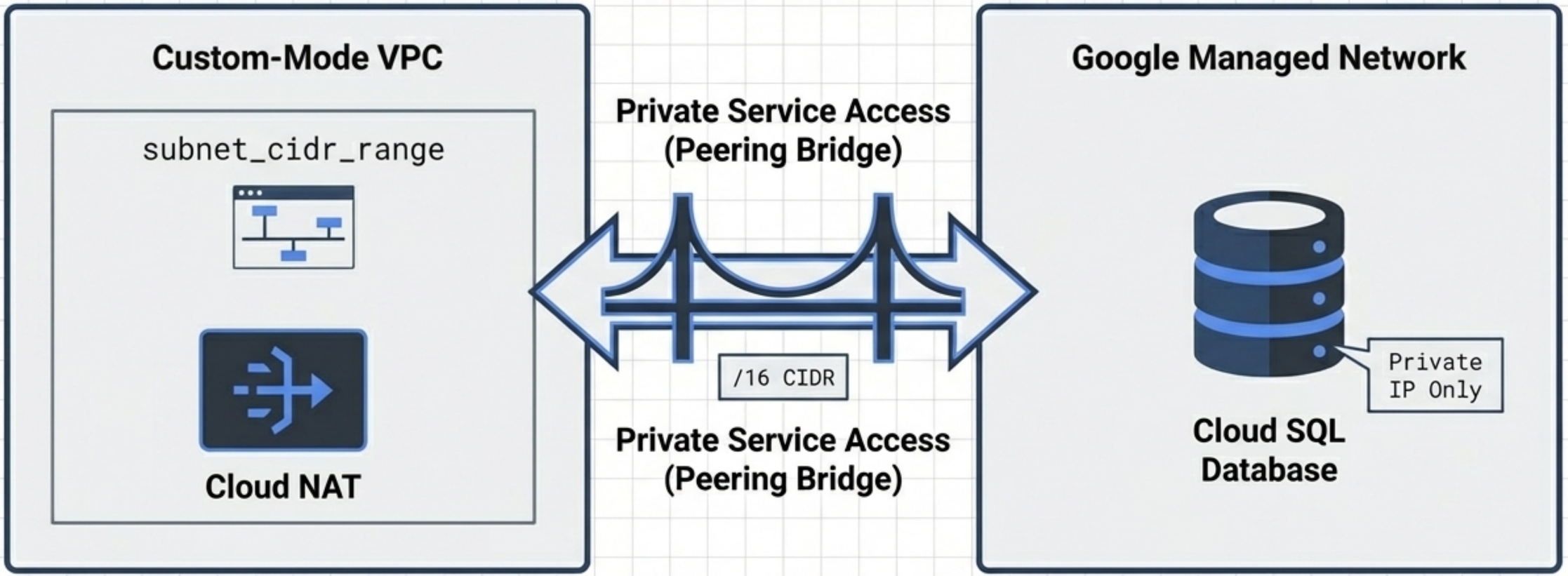


Google Workspace Group
(platform-team@)

Change membership in Cloud Identity; effective GCP access propagates automatically without touching IAM.

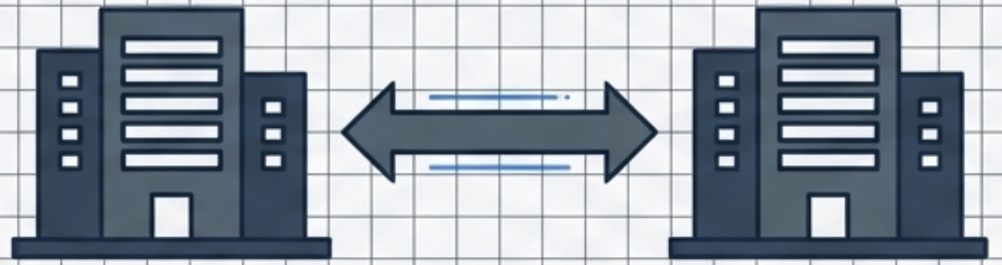
Google Cloud

The Network Foundation & Private Access



Private Service Access (PSA) creates a VPC peering connection. The database receives *only* a private IP, remaining entirely shielded from the public internet.

Geography & High Availability

ZONAL	REGIONAL
	
Characteristics: Single-zone, lower cost, ideal for Development/Testing.	**Characteristics:** Multi-zone HA, synchronous cross-zone replication, ideal for Production.
`postgres_database_availability_type = ZONAL` `filestore_tier = BASIC`	`postgres_database_availability_type = REGIONAL` `filestore_tier = ENTERPRISE`

Console Verification Loop: Check GCP Products by Region before setting the `availability_regions` variable to prevent deployment failures.

Activating the Environment: APIs & Quotas

The Prerequisites

>35 APIs Auto-Enabled by RAD

☑	Compute Engine API
☑	Kubernetes Engine API
☑	Cloud Run Admin API
☑	Secret Manager API

The Constraints

Understand per-project limits and how to request increases before workloads fail.

Module Architecture & Quota Matrix

	Services GCP	App CloudRun	App GKE
Primary Function	Shared infrastructure layer	Serverless containerized apps	Kubernetes workloads via Autopilot
Dedicated SAs Provisioned	Cloud Build, NFS, Workload SAs	Cloud Run Service SA, Cloud Build SA	GKE Workload SA, Cloud Build SA
Specific Quotas Stressed	Compute Engine IPs, Artifact Registry storage	Global external IPs, Cloud Run instance count/region	Autopilot pod vCPUs and memory/region

The Observability Stack

Dashboards

Tracks request counts, instance scaling, and GKE replica status.

Alert Policies

`alert_cpu_threshold`
`notification_alert_emails`

MQL-based alerts for CPU saturation, disk utilization, and p95 latency.

Uptime Checks

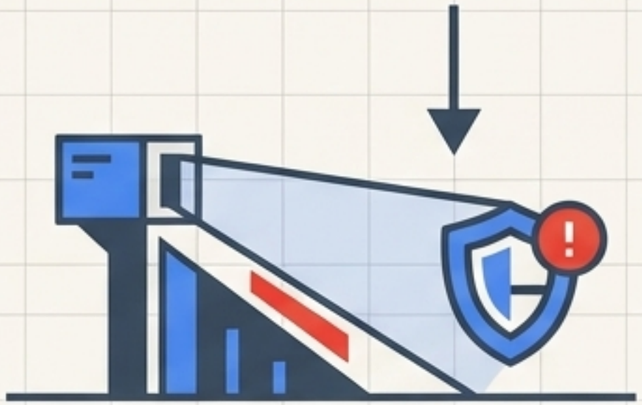
`uptime_check_config`

Global synthetic pings verifying application endpoint health.

Auditing at Scale: Cloud Asset Inventory & Gemini

`type: sqladmin.googleapis.com/Instance`

Asset API continuously indexes every provisioned resource.



Security Command Center (SCC) detecting a misconfiguration.

`enable_security_command_center`

Routing finding to Pub/Sub alert topic.

`enable_scc_notifications`

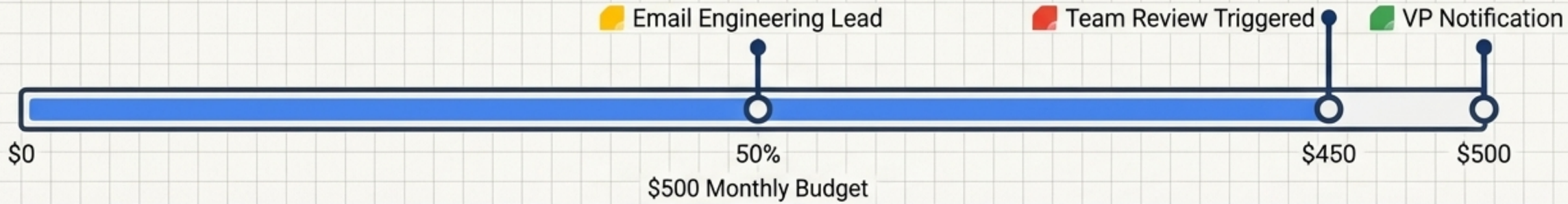
Gemini Cloud Assist enables natural-language querying of monitoring data and alert policies.

Billing Foundations: Linking & Guardrails

The Link

`billing_account_id` is a strict prerequisite for enabling quota-consuming paid APIs (GKE, Cloud SQL).

The Guardrail

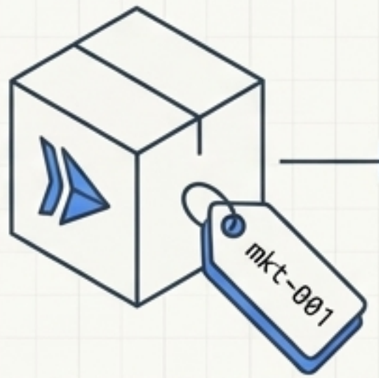


Cost Levers

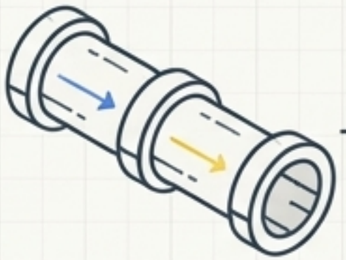
- Scale-to-zero (`min_instance_count = 0`) and infrastructure consolidation (`create_network_filesystem = true`) act as active cost reduction strategies.

The Chargeback Workflow

```
resource_labels = {
  cost-center = "mkt-001"
}
```



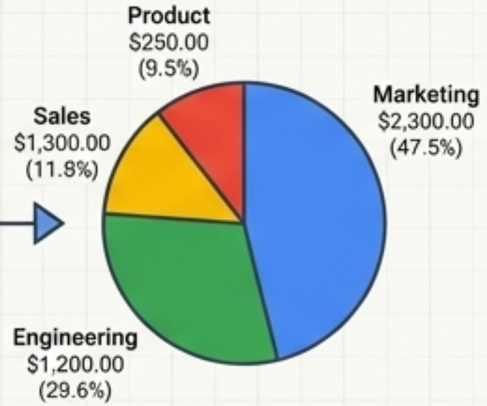
Cloud Run Instance
Roboto Regular



Cloud Billing Export
Roboto Regular

```
SELECT SUM(cost)...
GROUP BY labels.value
WHERE labels.key = "cost-center"
```

BigQuery
Roboto Regular



Spend perfectly attributed by business unit without requiring separate GCP projects.