Taking Anthos and AlloyDB for a Multicloud ride

Sri Rajan
Senior Principal Architect

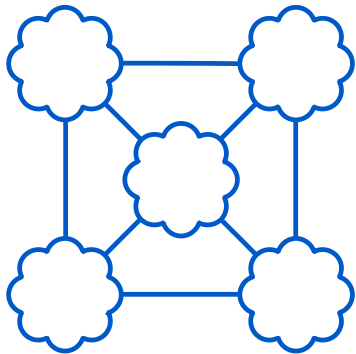**rackspace** technology® | **FAIR**
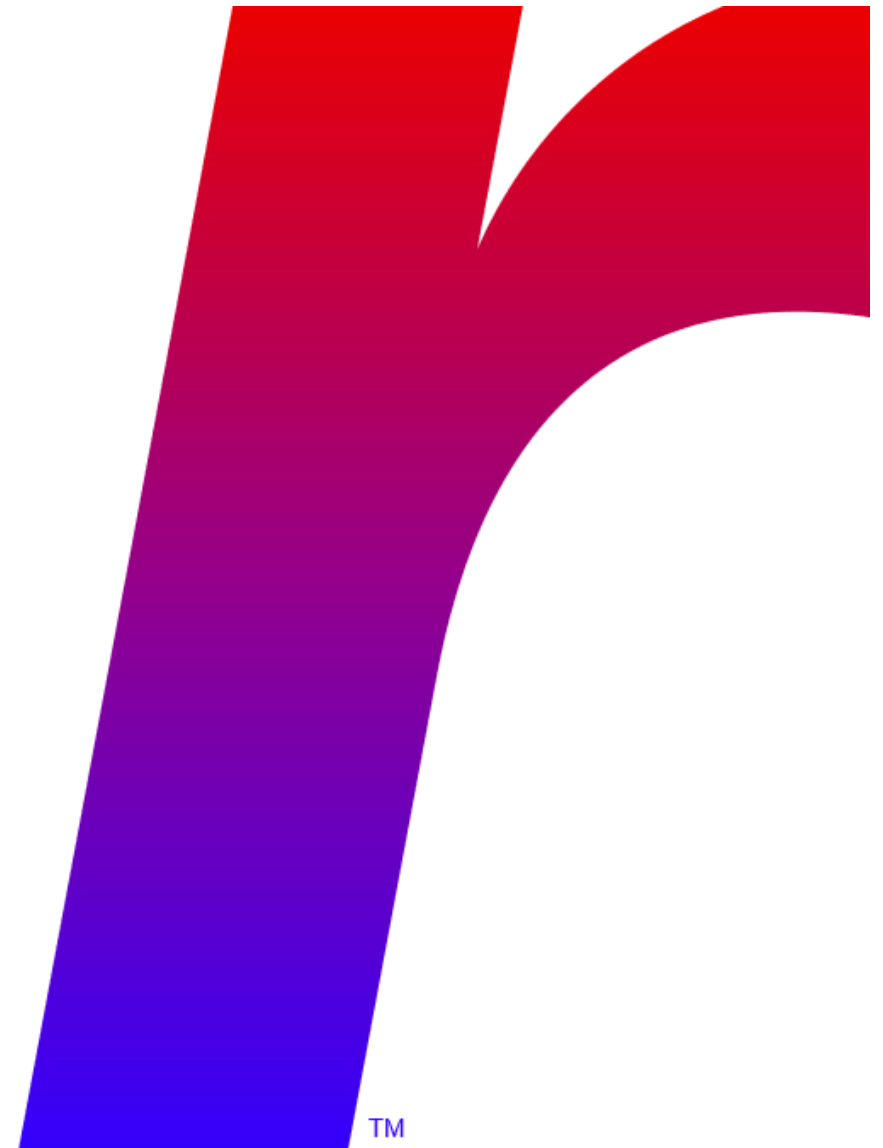
Next 15 minutes

Why Multicloud?

A reference architecture walkthrough

How does Google Cloud differentiate?

Some takeaways

rackspace technology. | F A I R

Why multicloud?

The cool kids are doing it ☺

Leverage different features, commercial models and regions

Disaster recovery

Go where your customers/ partners are

Insert image about analyst claims about Multicloud

rackspace technology | FAIR

But is it easy?

YEAH... IF YOU COULD GO AHEAD AND SETUP OUR DEV, STAGE, PROD ENVIRONMENTS IN A MULTI-CLOUD

THAT WOULD BE GREAT
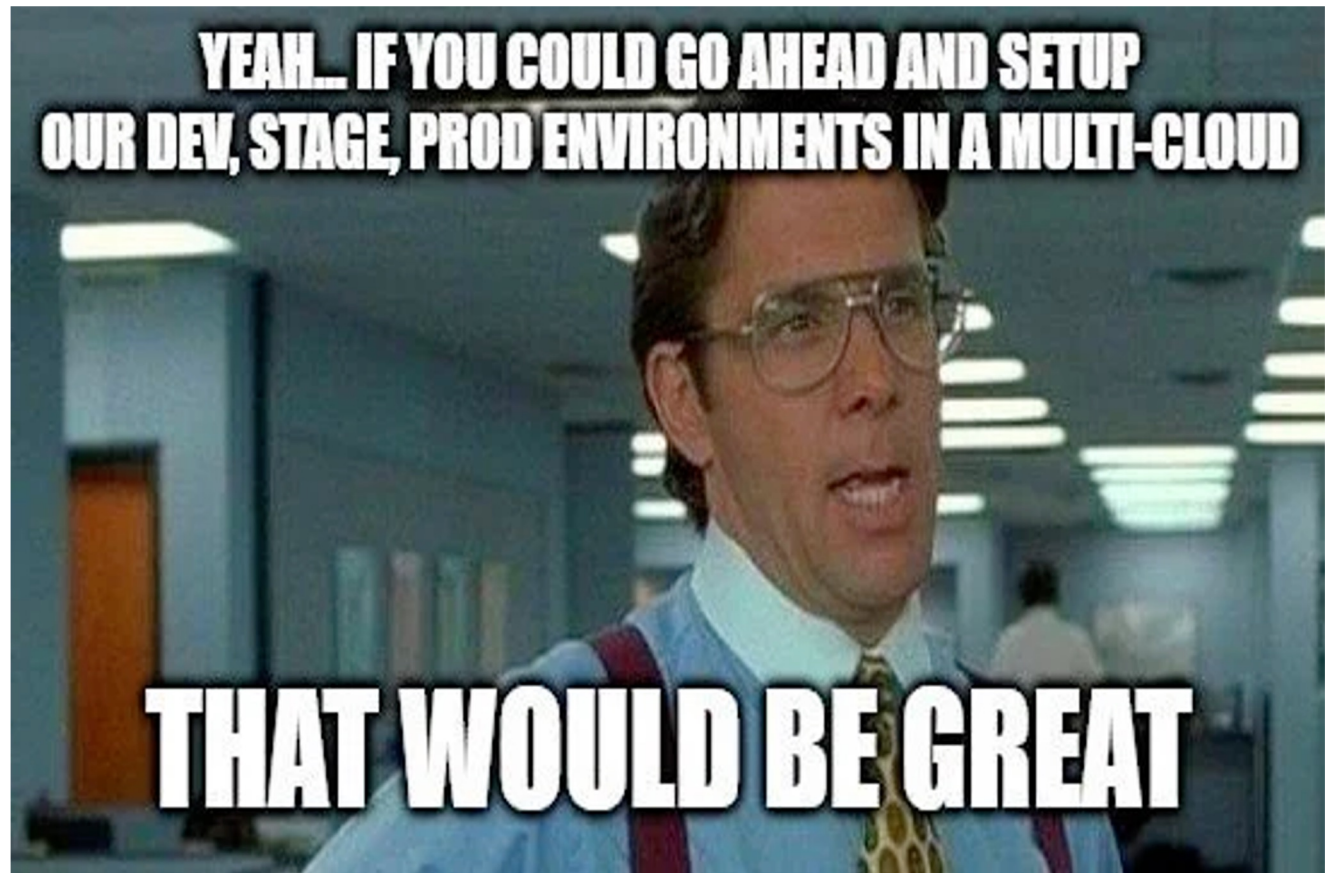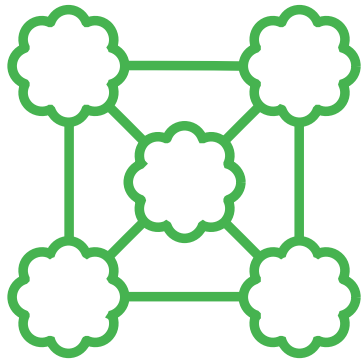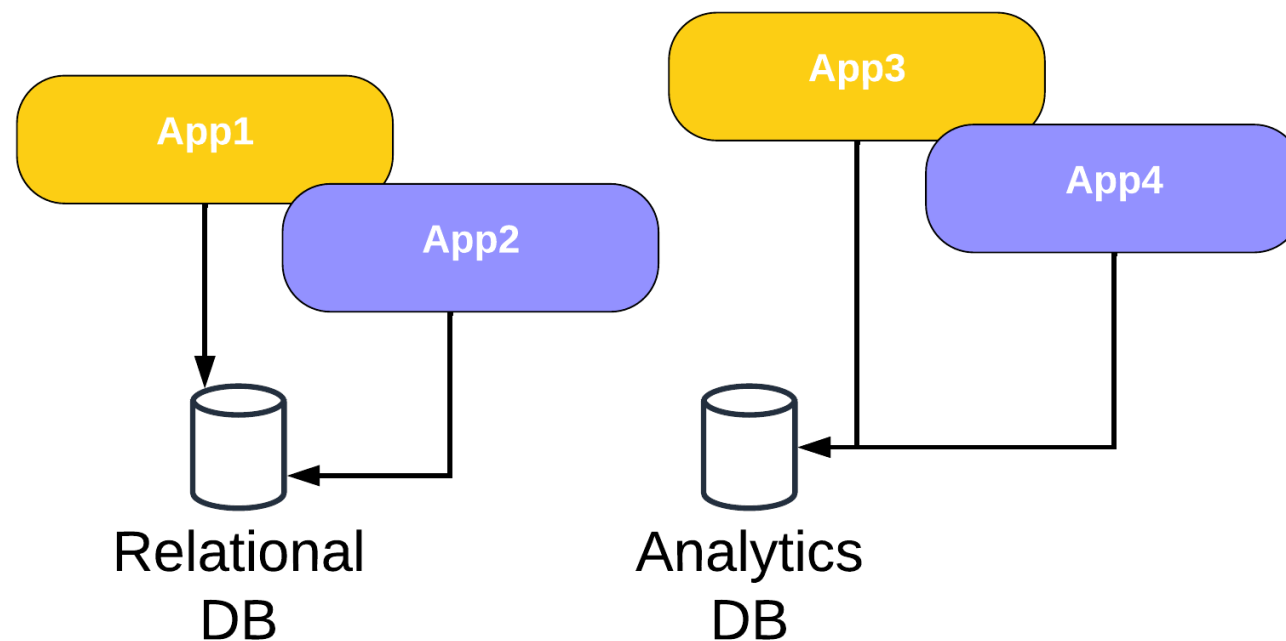
But **Google Cloud** is trying the best !!

Lots of open
themed technologies

Some key product
and solutions in the
last 12-18 months

"For now, what is important is not finding
the answer, but looking for it."

- Douglas R. Hofstadter, *Gödel, Escher, Bach: An Eternal Golden Braid*

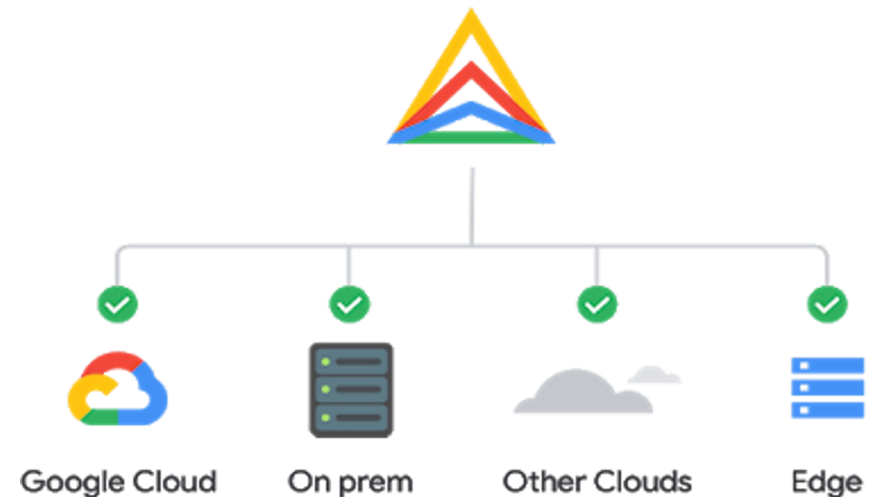# Let's begin the ride !

App1

App2

App3

App4

Relational
DB

Analytics
DB

Building Block #1 - Anthos

- Multicloud Managed Kubernetes
  - Attach feature for EKS/AKS

- Excellent features
  - GitOps for app config management
  - Multi cluster fleet management
  - Operations
  - Security

Google Cloud   On prem   Other Clouds   Edge

Building Block #1 - Anthos

Git Repo

Your application

k8s config

GKE

config mgmt
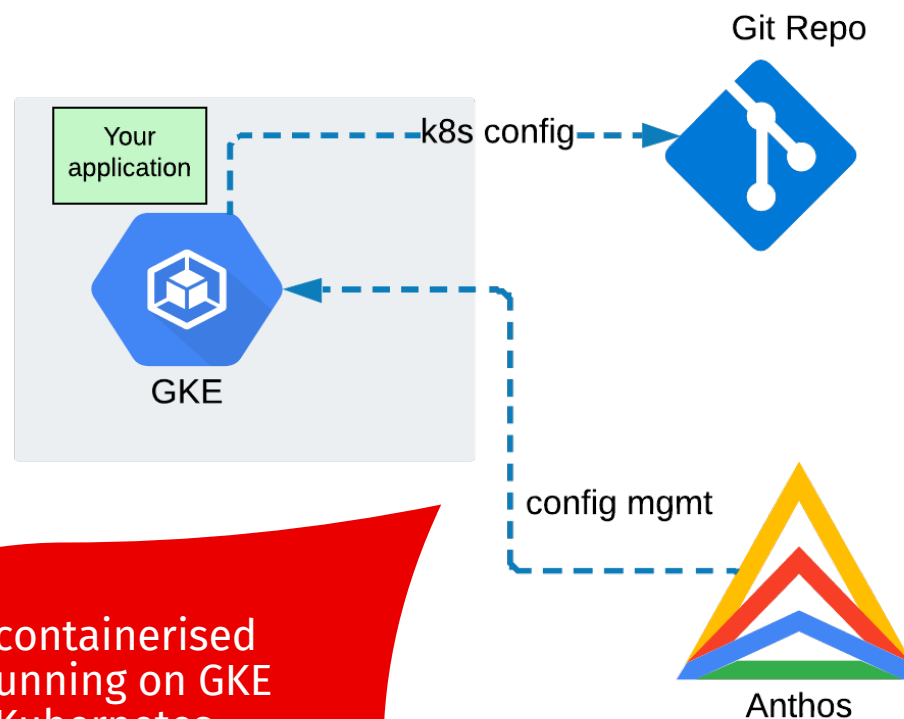
Anthos

- Your containerised app running on GKE
- Your Kubernetes configuration in Github with Anthos Config Management

rackspace technology. | **FAIR**

Building Block
#1 - Anthos

Git Repo

Your application
—k8s config——→
——k8s config——

GKE

config mgmt   config mgmt

Anthos

Your application

Kubernetes cluster mgd by Anthos

ENV1

Google Cloud

ENV2

aws
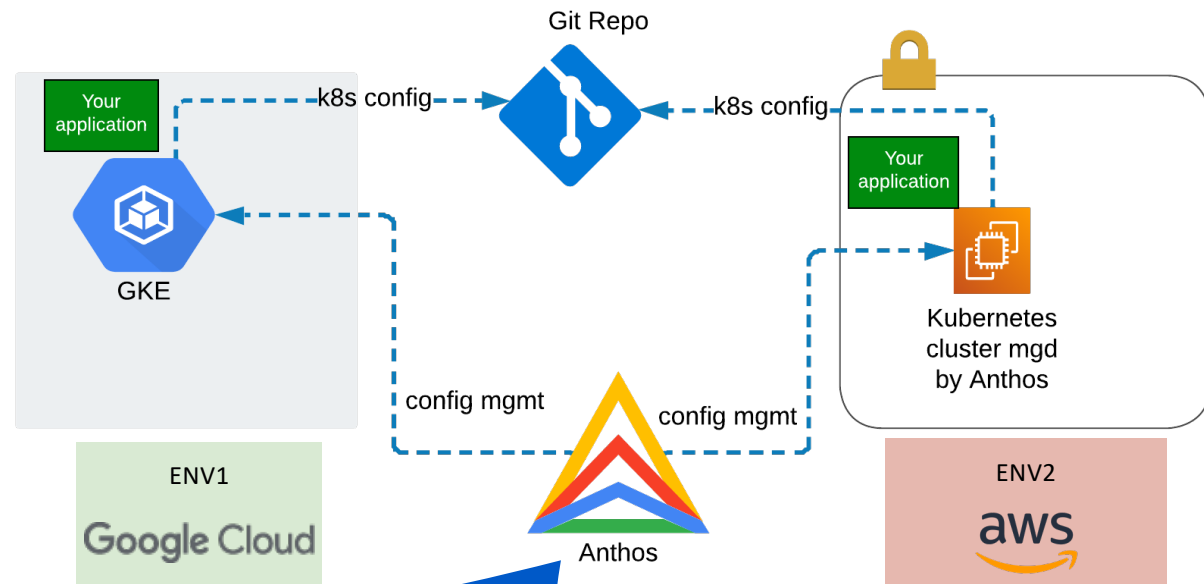
- Easy mirrored setup on AWS
- Consistent Kubernetes management with Anthos

rackspace
technology® | F A I R

Building Block #2 - AlloyDB
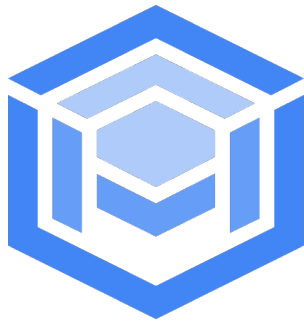
- Postgres compatible relational database
- New entry to Google Cloud
- Omni version for other clouds and on-premise

AlloyDB for PostgreSQL

Intelligent database storage designed and optimized for PostgreSQL

Zone one	Zone two	Zone (any)
Primary	Failover replica	Read pool node
optimized PostgreSQL	optimized PostgreSQL	optimized PostgreSQL
Analytics Accelerator / Cache	Analytics Accelerator / Cache	Analytics Accelerator / Cache

Only Log Writes   No BLOCK Writes

Intelligent Database Storage Engine

Google's Distributed File System - Colossus

Google I/O

rackspace technology | FAIR

Building Block #2 - AlloyDB

Your Relational Data

AlloyDB Primary

Read Replicas in other regions

Private Subnet

- Relational Data with AlloyDB
- Fully managed on Google Cloud

rackspace technology. | FAIR

Building Block #2 - AlloyDB

ENV1

Google Cloud

AlloyDB Primary

Your Relational Data

Read Replicas in other regions

Private Subnet

optional replication

ENV2

aws

Your Relational Data

Alloydb omni Primary

Alloydb omni Read Replicas

Private Subnets

- AlloyDB x 2
- Omni on AWS (in Preview)
- Partially managed
- Replication

rackspace technology® | F A I R

Building Block #3 - Big Query

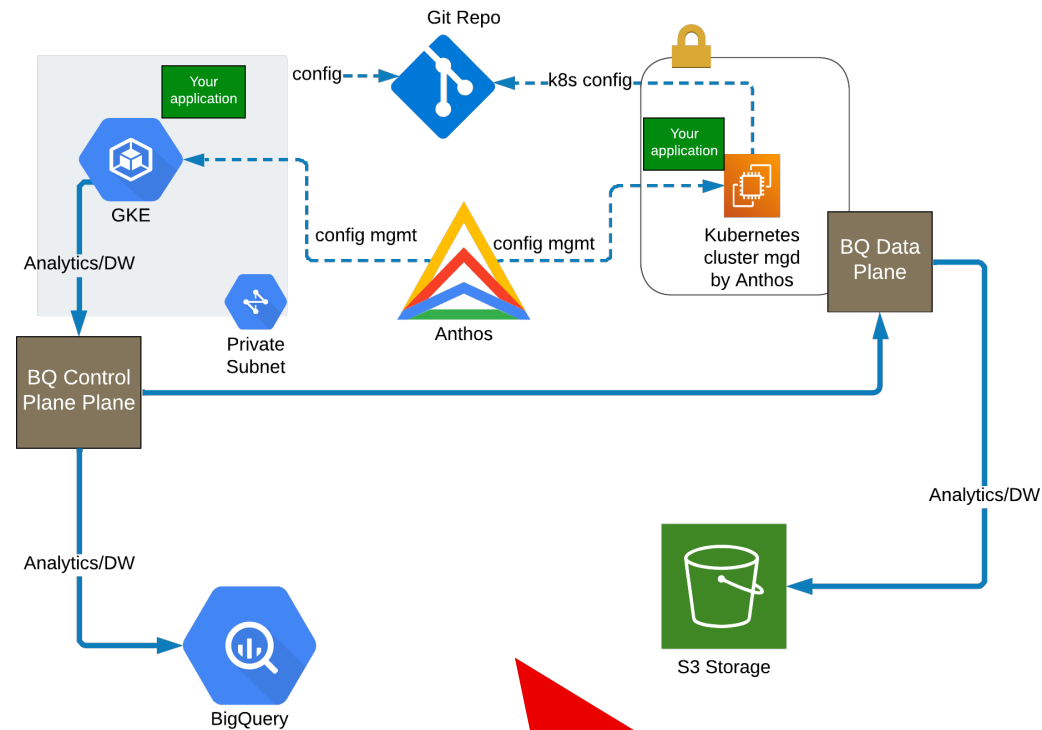- Powerful petabyte-scale analytics with inbuilt ML
- BQ Omni
  - Stateless compute
  - Data in AWS S3 or Azure Blob
- Looker Integration

Google Cloud   Other Public Cloud

Query Engine

Anthos Clusters managed by BigQuery

Building Block #3 - Big Query

Git Repo

config → ← k8s config

Your application

GKE

Analytics/DW

Private Subnet

config mgmt   config mgmt

Anthos

Your application

Kubernetes cluster mgd by Anthos

BQ Data Plane

BQ Control Plane Plane

Analytics/DW
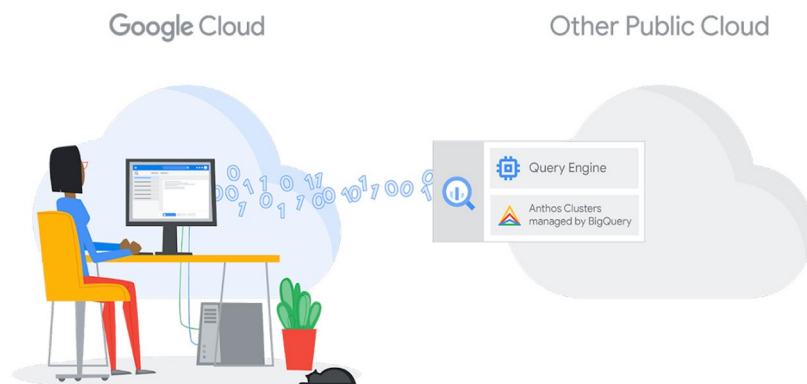
Analytics/DW

BigQuery

S3 Storage

- **Multicloud analytics with local storage and BigQuery Omni**

rackspace technology® | FAIR

The full design

- Applications deployed across Google Cloud and AWS using GitOps delivered by Anthos Config Management.

- An consistent database layer using Postgres compatible AlloyDB.

- An storage model using Google Cloud Storage and Amazon S3 but served by Big Query

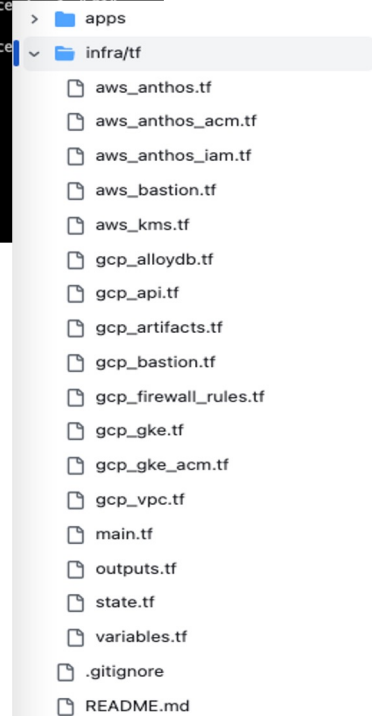- Necessary cloud-vendor-native constructs like VPC and Load balancers.
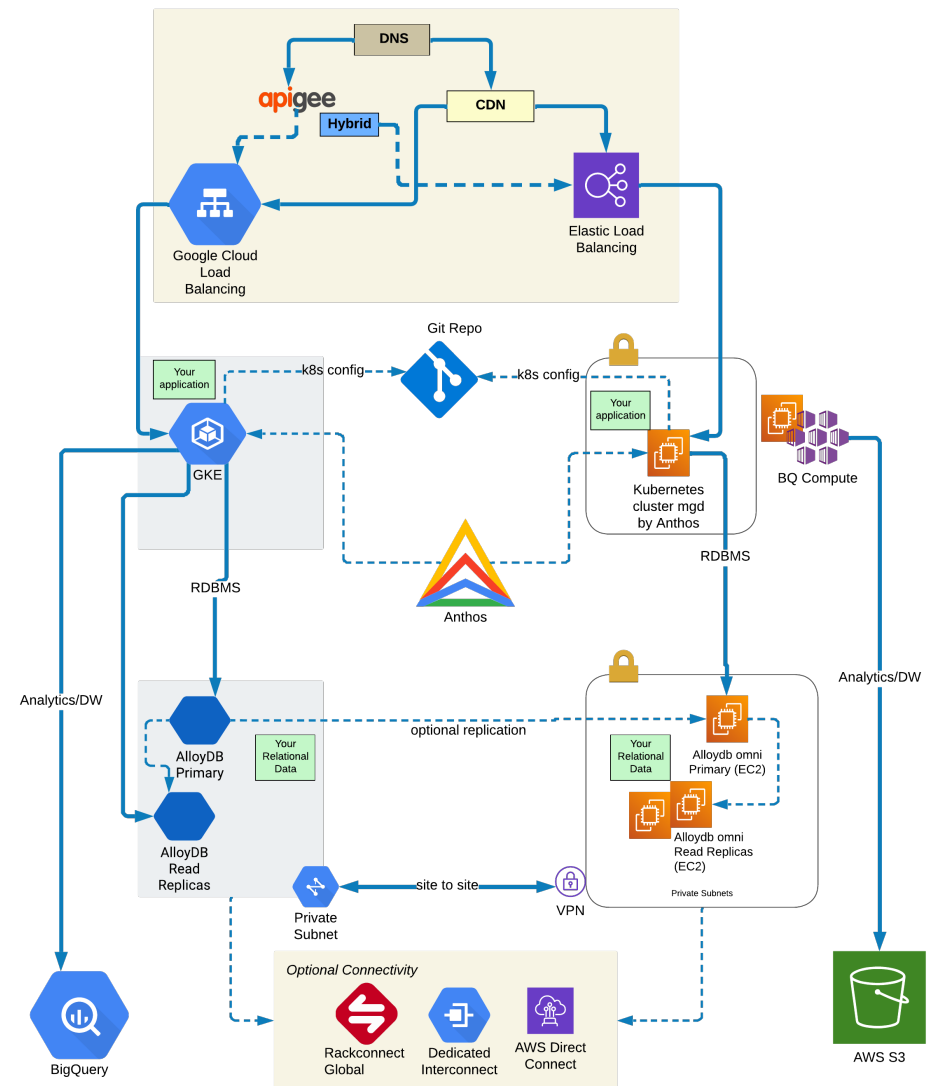
Beyond pictures

Apply complete! Resources: 131 added, 0 changed, 0 destroyed.

Outputs:

```
bigquery_omni_role = "arn:aws:iam::844054940671:role/bq-omni-connection"
env1_alloydb_helper_ip = "35.221.42.171"
env1_bastion_ip = "34.150.138.160"
env1_cluster_location = "us-east4"
env1_cluster_name = "env1-clu01"
env1_db_prim_id = "projects/gcp-mc-demo01/locations/us-east4/clusters/env1-clu01/instance
env1_db_prim_ip = "10.212.0.2"
env1_db_read_id = "projects/gcp-mc-demo01/locations/us-east4/clusters/env1-clu01/instance
env1_db_read_ip = "10.212.0.5"
env2_anthos_api_role_arn = "arn:aws:iam::844054940671:role/anthos-api-role"
env2_anthos_cp_role_arn = "arn:aws:iam::844054940671:role/anthos-cp-role"
env2_anthos_np_role_arn = "arn:aws:iam::844054940671:role/anthos-np-role"
env2_bastion_ip = "54.234.189.146"
env2_db_prim_ip = "10.1.77.87"
env2_db_prim_public_ip = "44.198.93.169"
myapp_repo_id = "projects/gcp-mc-demo01/locations/us-east4/repositories/myapp"
util_repo_id = "projects/gcp-mc-demo01/locations/us-east4/repositories/util"
```

> 📁 apps
∨ 📁 infra/tf
  📄 aws_anthos.tf
  📄 aws_anthos_acm.tf
  📄 aws_anthos_iam.tf
  📄 aws_bastion.tf
  📄 aws_kms.tf
  📄 gcp_alloydb.tf
  📄 gcp_api.tf
  📄 gcp_artifacts.tf
  📄 gcp_bastion.tf
  📄 gcp_firewall_rules.tf
  📄 gcp_gke.tf
  📄 gcp_gke_acm.tf
  📄 gcp_vpc.tf
  📄 main.tf
  📄 outputs.tf
  📄 state.tf
  📄 variables.tf
  📄 .gitignore
  📄 README.md

- Deployment using Terraform
- Some glue using kubectl

Code and reference at https://github.com/rax-incubate/gcp-mc-demo

rackspace technology® | F A I R

Example App

Environment:env2-aws

Tile	Start Year
A Thin Life	2018
Holy Hollywood	2021
Bachelor Trip	2012
Take Out	2022
Party Crashers	2012
Stan	2011
Bamboo Shark	2011
Persona Au Gratin	2012
Monkey Man	2011
Have You Seen Me?	2016
The Incredible Burt Wonderstone	2013
Jack and Jill	2011
The Do-Deca-Pentathlon	2012

Environment:env1-gcp

Tile	Start Year
A Thin Life	2018
Holy Hollywood	2021
Bachelor Trip	2012
Take Out	2022
Party Crashers	2012
Stan	2011
Bamboo Shark	2011
Persona Au Gratin	2012
Monkey Man	2011
Have You Seen Me?	2016
The Incredible Burt Wonderstone	2013
Jack and Jill	2011
The Do-Deca-Pentathlon	2012
The Babymakers	2012
Naked Run	2011
6 Month Rule	2011
The Nightclub Days	2012
The Wedding Ringer	2015

Code and reference at https://github.com/rax-incubate/gcp-mc-demo

Configuration Sync

DASHBOARD   PACKAGES PREVIEW   SETTINGS

Reconciliation status ?

2 Packages

- 2 current
- 0 in progress
- 0 failed
- 0 unknown

Synchronisation status ?

2 Packages

- 2 synced
- 0 pending
- 0 reconciling
- 0 stalled
- 0 error
- 0 unknown

Top package issues

Name	Reconcile issues	Sync issues
No issues to display		

VIEW STATUS BY PACKAGE →

Top cluster issues

Name	Reconcile issues	Sync issues
No issues to display		

VIEW STATUS BY CLUSTER →

rackspace technology | FAIR

Code and reference at https://github.com/rax-incubate/gcp-mc-demo

Package view

Code and reference at https://github.com/rax-incubate/gcp-mc-demo

Security view

Filter | Namespace : myapp ⊗ | Enter property name or value

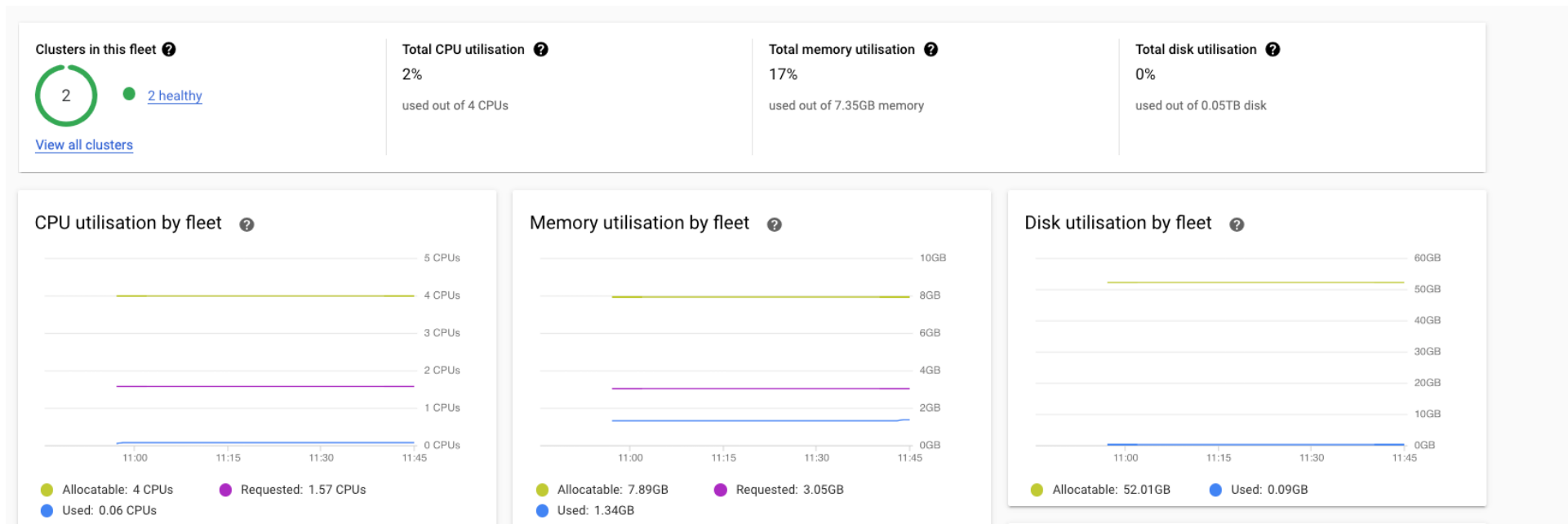| Resource name ↑	Group	Namespace	Kind	Constraint	Status
myapp-69f7c69596-64mtk		myapp	Pod	policy-essentials-v2022-psp-pods-must-run-as-nonroot	⚠ Container myapp is attempting to run without a required securityContext/runAsNonRoot or securityContext/runAsUser != 0
myapp-69f7c69596-64mtk		myapp	Pod	policy-essentials-v2022-psp-allow-privilege-escalation	⚠ Privilege escalation container is not allowed: myapp
myapp-69f7c69596-64mtk		myapp	Pod	policy-essentials-v2022-psp-seccomp-default	⚠ Seccomp profile is not allowed, pod: myapp-69f7c69596-64mtk, container: myapp, Allowed profiles: ["runtime/default", "doc...
myapp-69f7c69596-64mtk		myapp	Pod	policy-essentials-v2022-psp-capabilities	⚠ container <myapp> is not dropping all required capabilities. Container must drop all of ["NET_RAW"] or "ALL"
myapp-69f7c69596-64mtk		myapp	Pod	policy-essentials-v2022-pods-require-security-context	⚠ securityContext must be defined for all Pod containers
myapp-69f7c69596-64mtk		myapp	Pod	policy-essentials-v2022-no-secrets-as-env-vars	⚠ Container <myapp> has secret defined as environment variable

Constraints

Your cluster was audited against the following constraints. Learn more ↗

Filter | Enter property name or value

Name ↑	Kind	Description
policy-essentials-v2022-no-secrets-as-env-vars	K8sNoEnvVarSecrets	
policy-essentials-v2022-pods-require-security-context	K8sPodsRequireSecurityContext	
policy-essentials-v2022-prohibit-role-wildcard-access	K8sProhibitRoleWildcardAccess	
policy-essentials-v2022-psp-allow-privilege-escalation	K8sPSPAllowPrivilegeEscalationContainer	
policy-essentials-v2022-psp-capabilities	K8sPSPCapabilities	
policy-essentials-v2022-psp-host-namespace	K8sPSPHostNamespace	
policy-essentials-v2022-psp-host-network-ports	K8sPSPHostNetworkingPorts	
policy-essentials-v2022-psp-pods-must-run-as-nonroot	K8sPSPAllowedUsers	

rackspace technology | FAIR

Code and reference at https://github.com/rax-incubate/gcp-mc-demo

Fleet Management

Clusters in this fleet ❓
2   ● 2 healthy
View all clusters

Total CPU utilisation ❓
2%
used out of 4 CPUs

Total memory utilisation ❓
17%
used out of 7.35GB memory

Total disk utilisation ❓
0%
used out of 0.05TB disk

CPU utilisation by fleet ❓

5 CPUs
4 CPUs
3 CPUs
2 CPUs
1 CPUs
0 CPUs
11:00   11:15   11:30   11:45

● Allocatable: 4 CPUs   ● Requested: 1.57 CPUs
● Used: 0.06 CPUs

Memory utilisation by fleet ❓

10GB
8GB
6GB
4GB
2GB
0GB
11:00   11:15   11:30   11:45

● Allocatable: 7.89GB   ● Requested: 3.05GB
● Used: 1.34GB

Disk utilisation by fleet ❓

60GB
50GB
40GB
30GB
20GB
10GB
0GB
11:00   11:15   11:30   11:45

● Allocatable: 52.01GB   ● Used: 0.09GB

Code and reference at https://github.com/rax-incubate/gcp-mc-demo

Some Takeaways

Multicloud is very much feasible with some design choices

Don't go for the lowest common denominator

Region selection is a tricky if you want to use Anthos and BQ Omni together

Cost of experimenting is roughly 400 USD per week for this reference design

Code and reference at https://github.com/rax-incubate/gcp-mc-demo

www.rackspace.com/cloud/google-cloud

BOOTH 217
Learn more about Rackspace

+

Foundry for AI by Rackspace (FAIR™)

+

Get AI generated stickers

Thank You