ENV: production | EXAM_WEIGHT: ~30% | SECTION: 02

The ACE Blueprint

Planning and Implementing Cloud Solutions

A HIGH-YIELD VISUAL STUDY GUIDE FOR THE GOOGLE CLOUD ASSOCIATE CLOUD ENGINEER

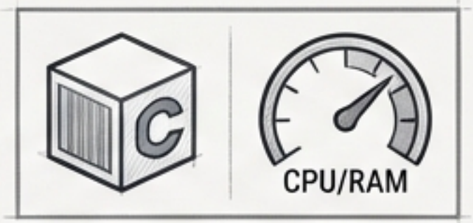
Declarative Inputs (RAD UI)

```
container_resources: CPU/Memory
```

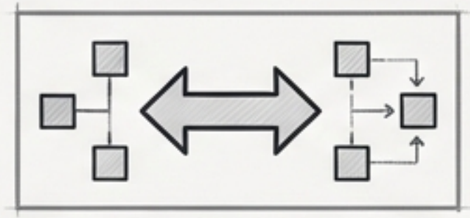
```
min_instance_count: 1
```

```
enable_cloud_armor: true
```

Provisioned Infrastructure (GCP Console)



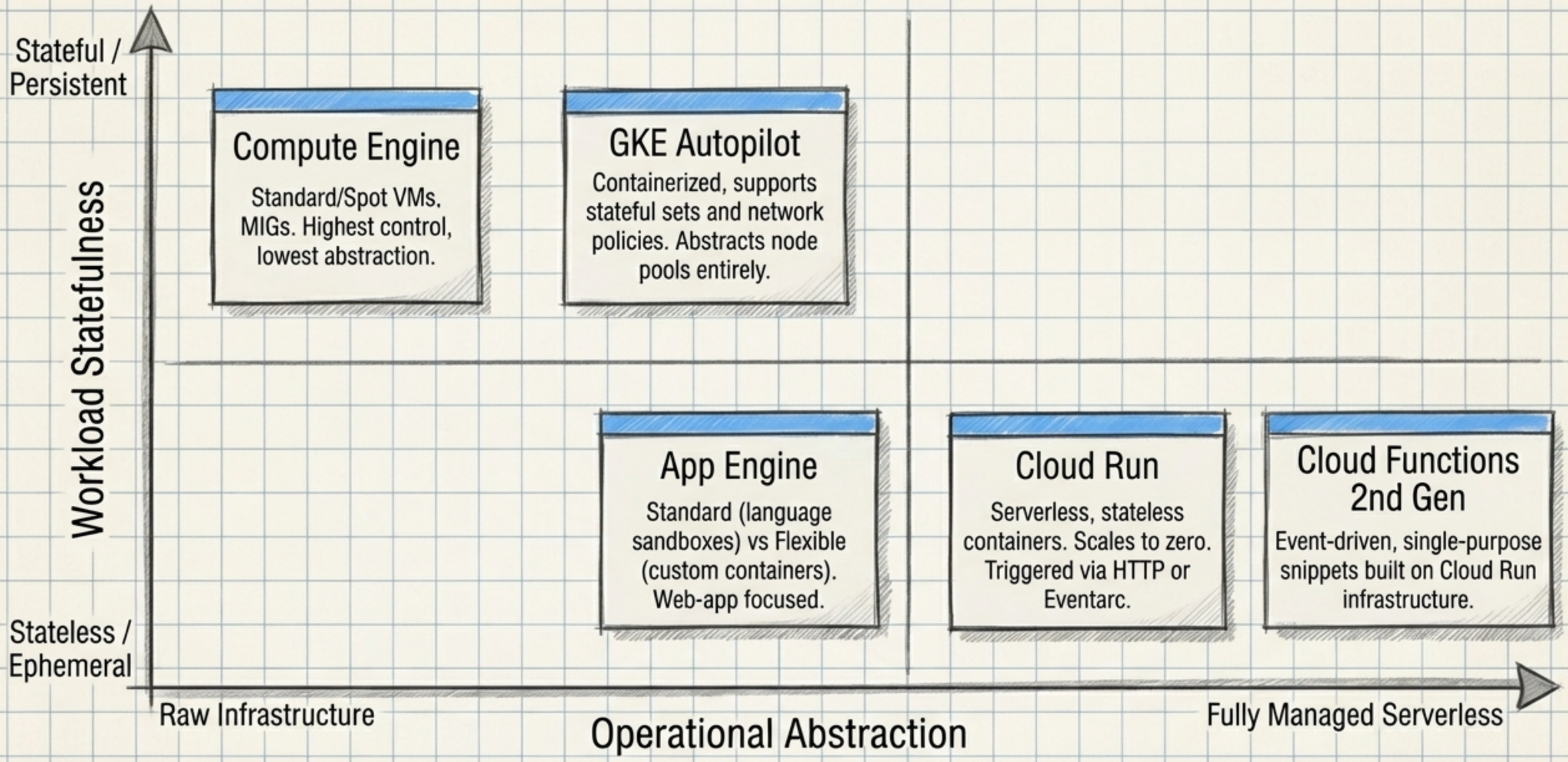
Cloud Run Revisions / GKE Workloads



Horizontal Pod Autoscaler (HPA)

Global External App Load Balancer + WAF

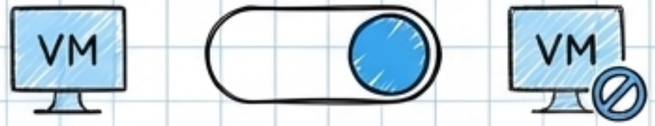
Infrastructure as Code abstracts the underlying complexity, but the ACE exam tests your mastery of the resulting reality.



Key Takeaway: Move right for operational efficiency.
Move up and left for customized state and granular control.

VM Fleet Diagnostics

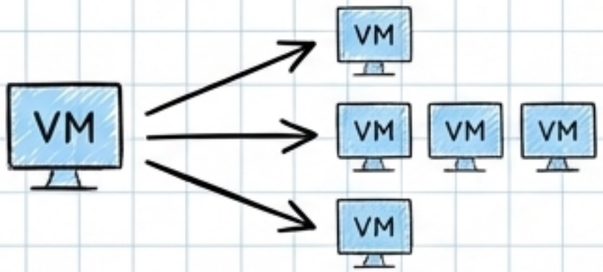
Standard vs Spot



Standard
Guaranteed uptime

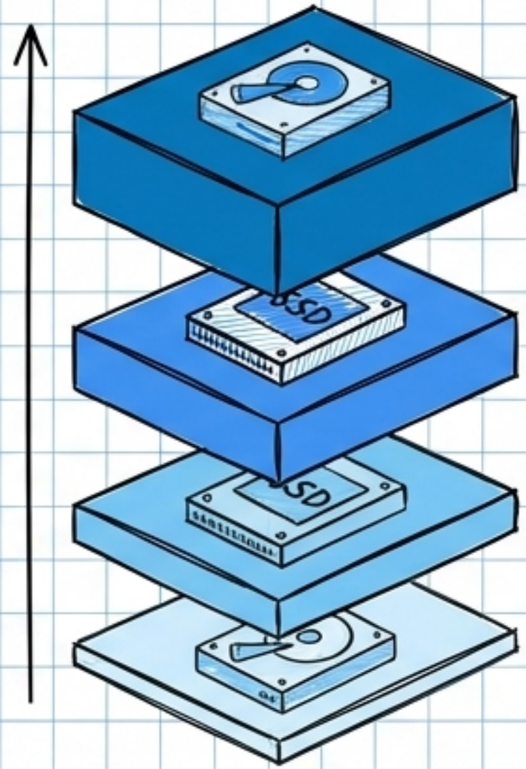
Spot
Lower cost, pre-emptible, strict availability policy

Managed Instance Groups (MIGs)



Autoscaling + Rolling Updates. Control maximum unavailable & surge count during template rollouts.

Block Storage Tiering



Hyperdisk
Next-gen storage (Extreme/Throughput). Independently configurable IOPS and capacity for advanced databases.

SSD (pd-ssd)
High-performance transactional workloads.

Balanced (pd-balanced)
SSD for standard OS disks.

Standard (pd-standard)
HDD for sequential backups.

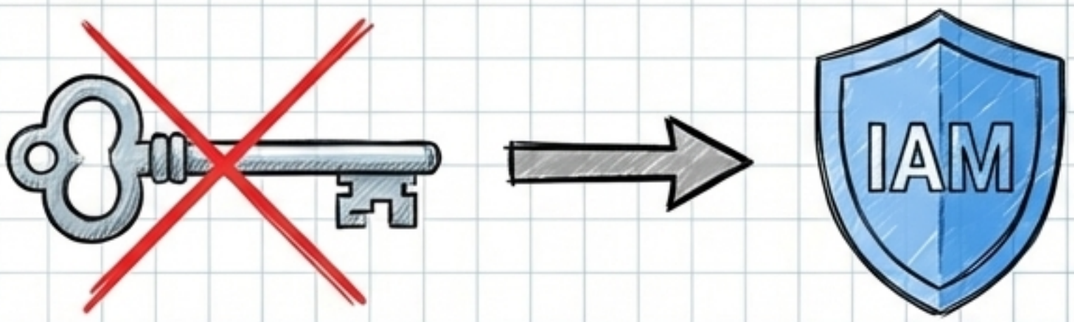
Note: Zonal vs. Regional PDs.

Regional synchronously replicates across two zones for High Availability.

Key Takeaway: Select the appropriate compute and storage tier based on workload criticality, performance requirements, and cost optimization strategies.

OS & Fleet Management

Access Architecture: OS Login



Project-level metadata **(enable-oslogin=true)**.
Replaces fragile SSH keys with IAM roles **(roles/compute.osLogin** & **roles/compute.osAdminLogin)**.
Google's recommended access method.

VM Manager Suite

OS Patch Management

Schedules automated patch jobs across fleets with defined rollout windows.

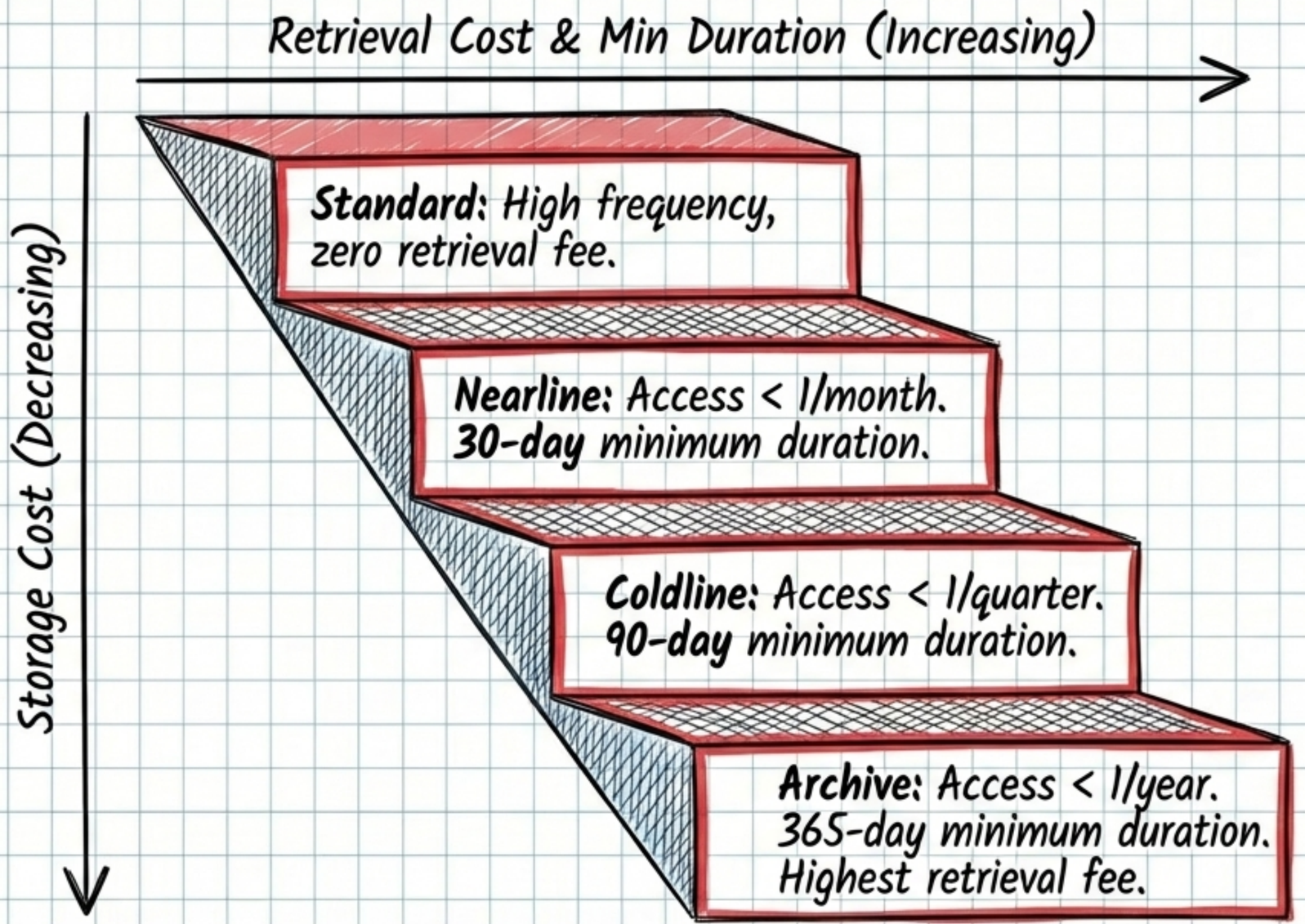
OS Configuration Management

Declaratively enforces desired state via OS policies.

OS Inventory

Collects installed package data across the entire project footprint.

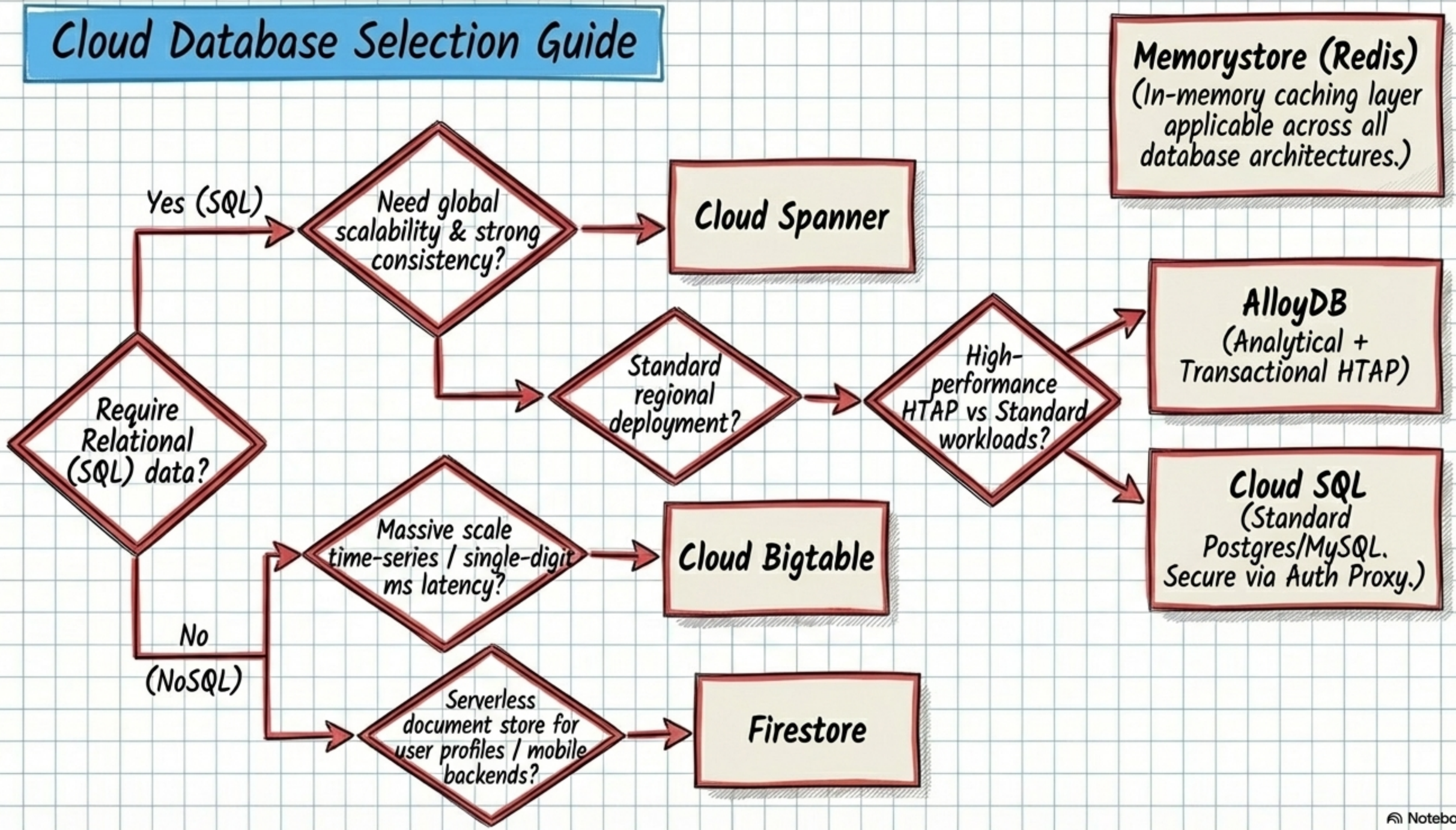
Object Storage Tiering & NFS



Network File Systems (NFS)

- **Cloud Filestore:** Fully managed NFS. Shares persistent files across containers.
- **NetApp Volumes:** Enterprise alternative for SAP/Oracle. Advanced snapshots, cloning, and SMB support.

Cloud Database Selection Guide



Architectural Data Pipeline: Ingestion, Processing & Analytics

Ingestion & Messaging

Pub/Sub

Decouples producers/consumers. Core backbone for event-driven async messaging.

Managed Kafka

Drop-in replacement for self-managed Apache Kafka.

Event Routing & Processing

Eventarc

Routes events (Pub/Sub, GCS audit logs) directly to Cloud Run targets.

Dataflow

Apache Beam-based serverless stream & batch processing (ETL, real-time enrichment).

The Analytics Hub

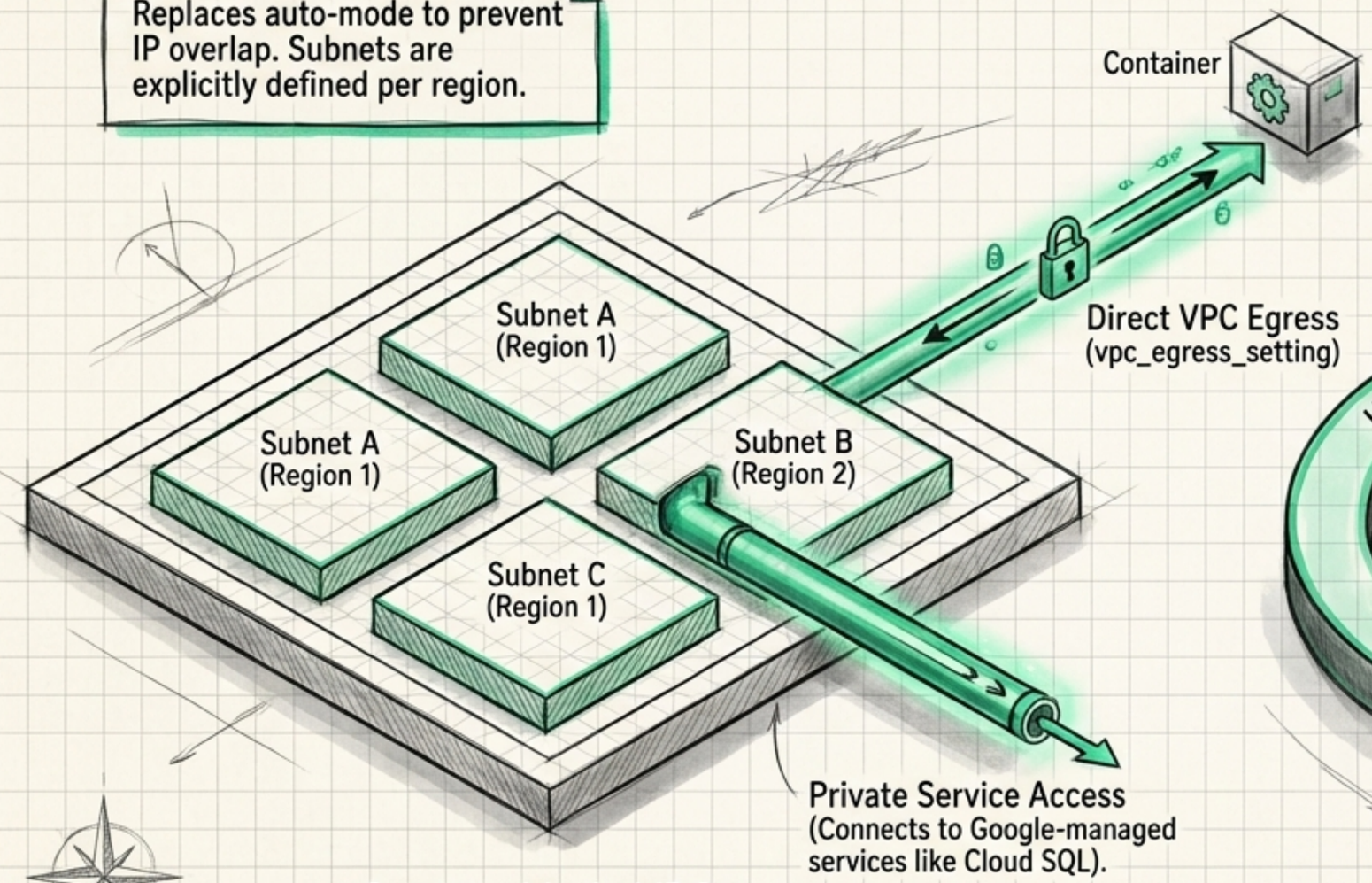
BigQuery

Serverless analytics. Ingests via Dataflow, native Pub/Sub subscriptions, or or direct loads.

Data Loading Mechanics: Transfer locally via **gcloud storage cp**, load to BigQuery via **bq load**, or automate cross-project replication via Storage Transfer Service.

VPC Architectures: Custom-Mode & Shared VPC

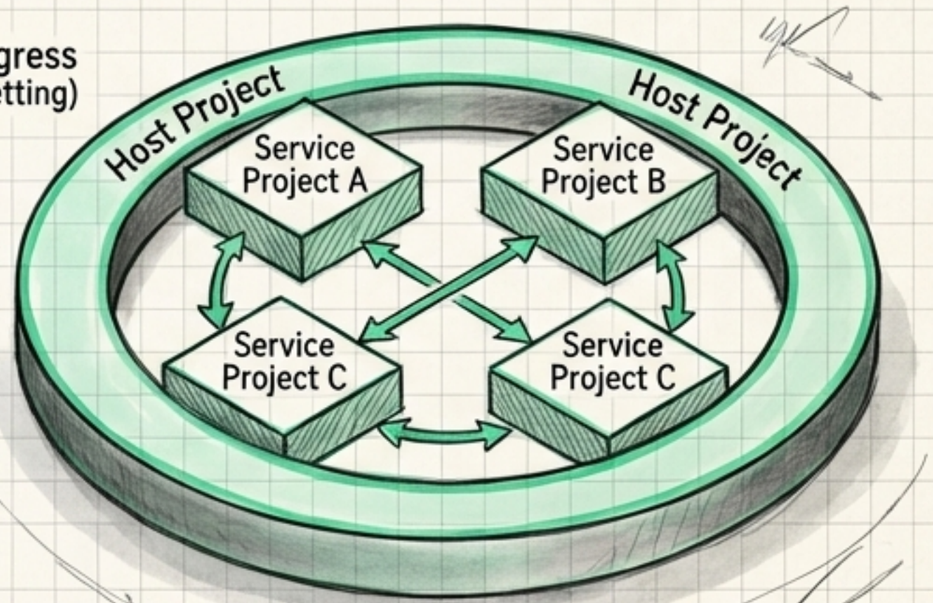
Replaces auto-mode to prevent IP overlap. Subnets are explicitly defined per region.



Custom-Mode VPC

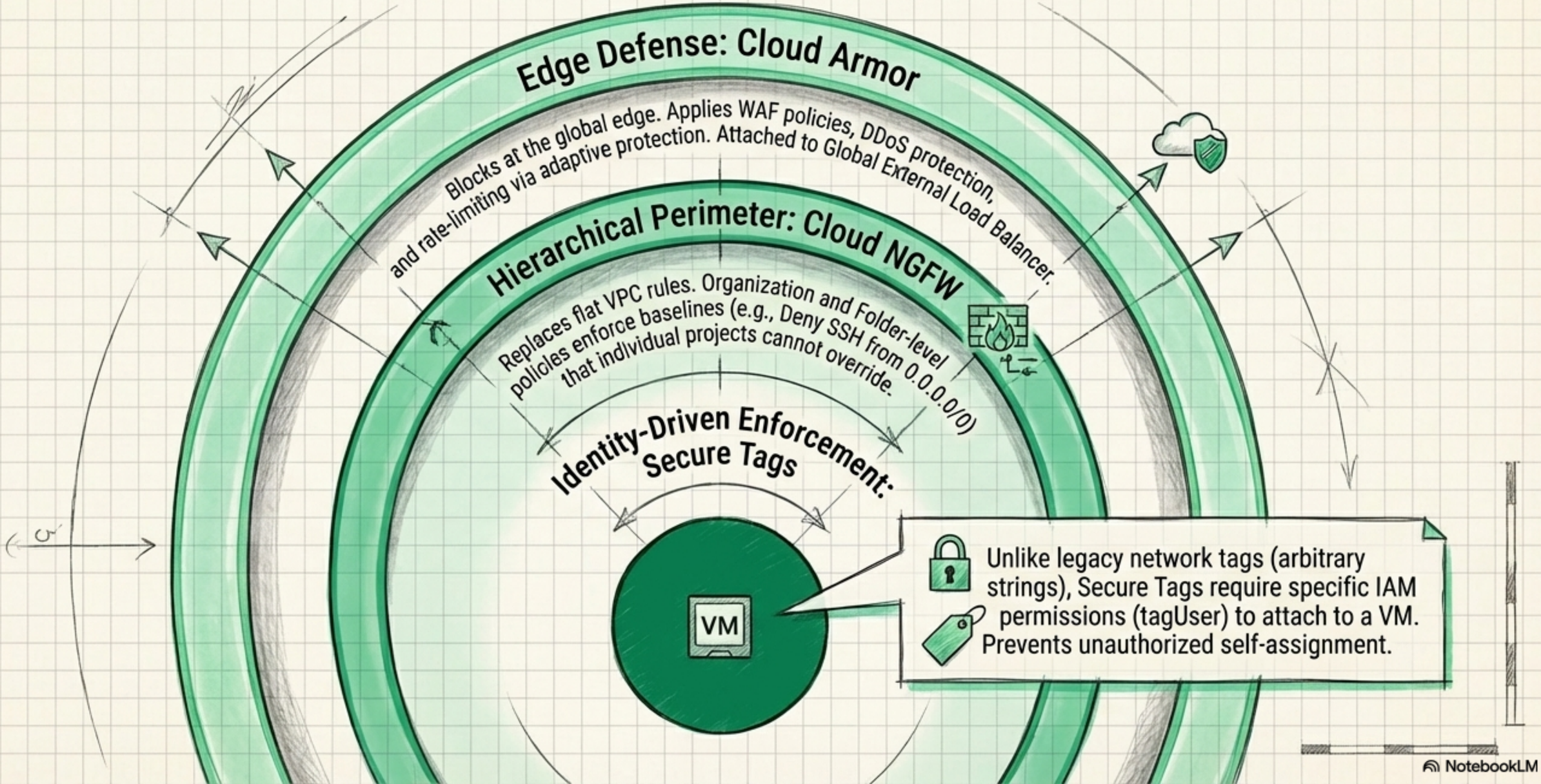
Host project owns the VPC network. Service projects attach to it.

Enables centralized network governance while separating application IAM boundaries.



Shared VPC Architecture

Architectural Defense: Cloud Security Perimeter



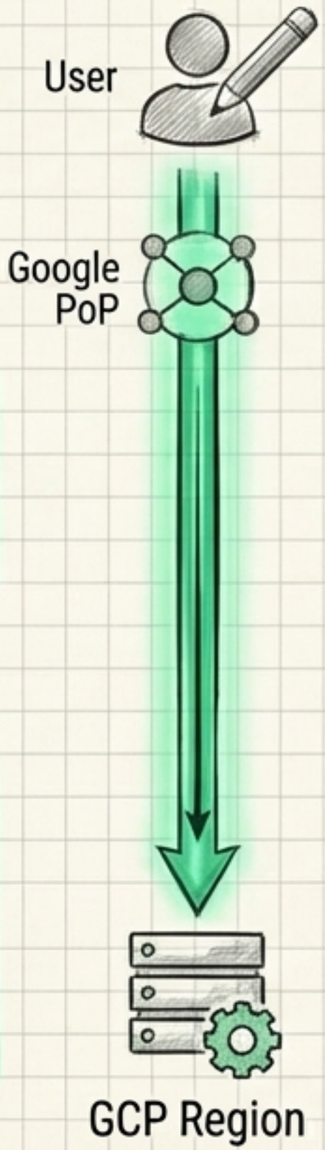
Network Tier Comparison: Premium vs. Standard

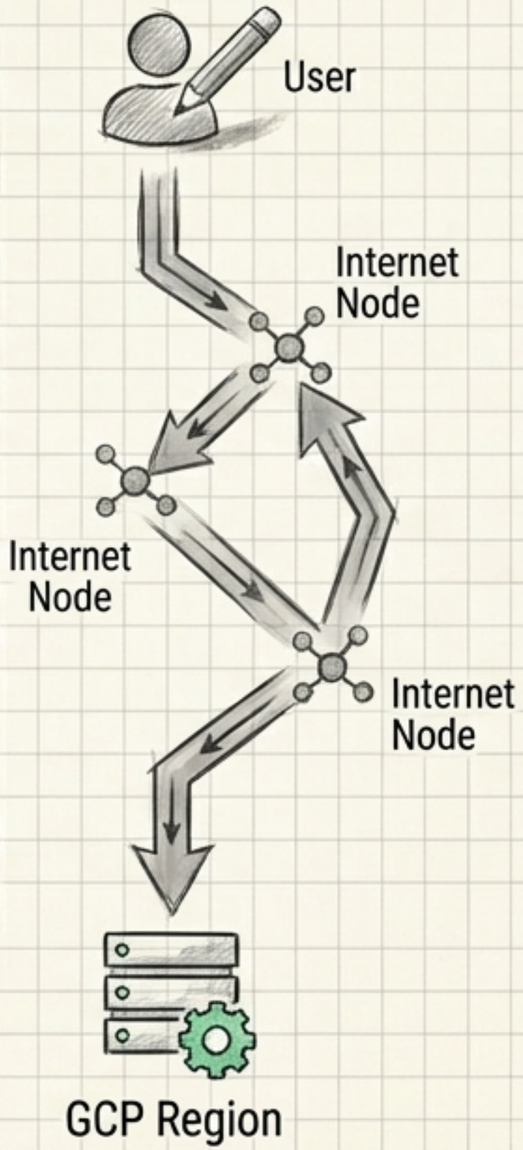
Premium Tier
(The Google Backbone)

Default tier. Traffic enters Google's network immediately. Required for Global External App Load Balancers and global Anycast IPs. Minimizes latency; highest SLA.

Global External Application Load Balancer

Terminates SSL globally on a single Anycast IP.
Routes traffic to Serverless NEGs (Cloud Run) or the Gateway API (GKE).

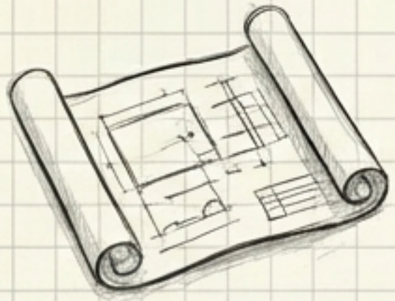




Standard Tier
(The Public Internet)

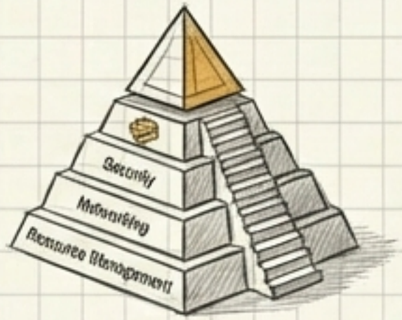
Lower cost. Traffic uses the public internet for the majority of the transit. No SLA equivalent to Premium. For non-latency-sensitive workloads.

Infrastructure as Code: Tooling Landscape & Strategy



Terraform
(The Core)

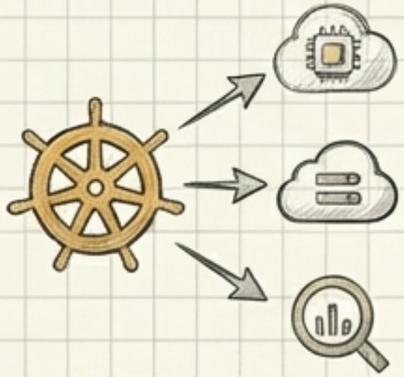
Declarative state management (terraform.tfstate) stored in versioned GCS buckets. terraform plan previews destructive changes. Lock providers to prevent breaking updates.



Fabric FAST
(The Enterprise Foundation)

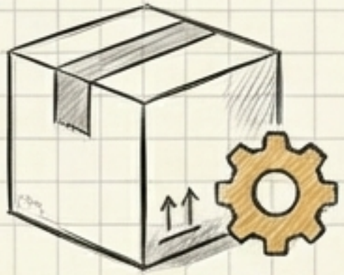
Google's opinionated Terraform framework. Bootstraps production landing zones in progressive stages (Resource Management -> Networking -> Security).

Config Connector
(Kubernetes Native)



Manages GCP resources directly as Kubernetes Custom Resource Definitions (CRDs). Enables unified GitOps pipelines using standard kubectl commands.

Helm
(App Packaging)



Kubernetes package manager. Bundles manifests (Deployments, Services, HPA) into versioned archives with environment-specific templating.

Essential Google Cloud CLI Tools

The Swiss Army Knife: gcloud

```
gcloud compute instances create ...
gcloud run deploy ...
```

Critical flag for scripting and exam scenarios: `--format='value(name)'`

GKE Mastery: kubectl

```
kubectl get pods
kubectl describe deployment
```

Deep Dive: `kubectl exec -it <pod> -- /bin/sh` (Opens a live shell inside a running container for debugging).

The Modern Data Mover: gcloud storage

```
gcloud storage buckets create gs://my-bucket
gcloud storage cp ./file.txt gs://my-bucket/
```

Replaces legacy gsutil. Offers faster parallel transfers.

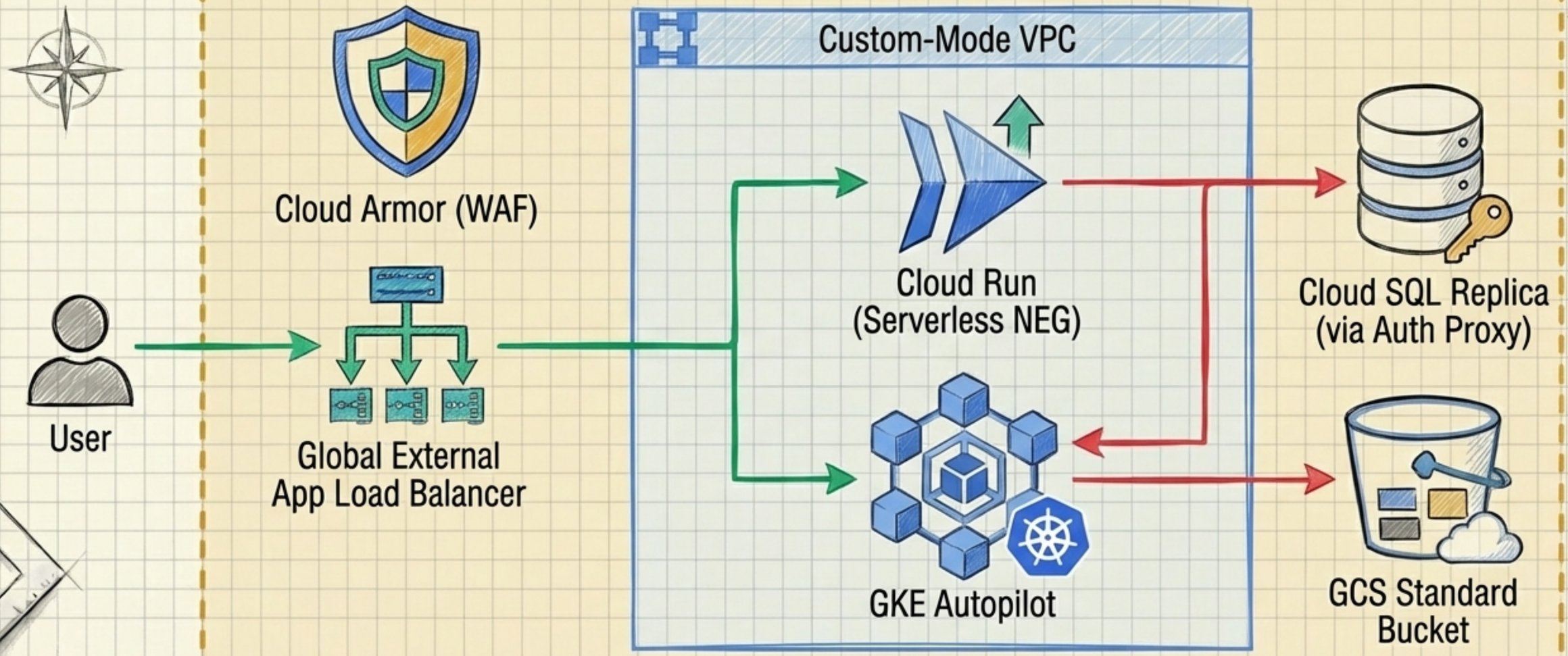
BigQuery CLI: bq

```
bq load ...
```

(Subtext: Imports data from GCS)

```
bq query --use_legacy_sql=false 'SELECT ...'
```

Provisioned idempotently via Terraform & Config Connector



The Holistic Cloud: Scalable compute, stateful persistence, and secure networking, entirely automated by code.

Compute

- [ ] Standard vs. Spot availability profiles.
- [ ] OS Login enablement vs legacy SSH.
- [ ] Serverless scaling bounds (min/max_instance_count).

Storage & Data

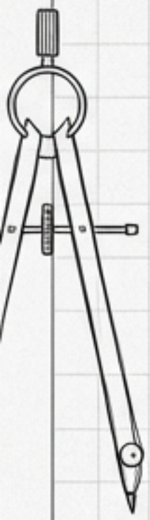
- [ ] GCS Storage Class minimum durations (30/90/365 days).
- [ ] Relational (Spanner/SQL) vs NoSQL (Bigtable/Firestore) use cases.
- [ ] Regional vs Zonal Persistent Disk mechanics.

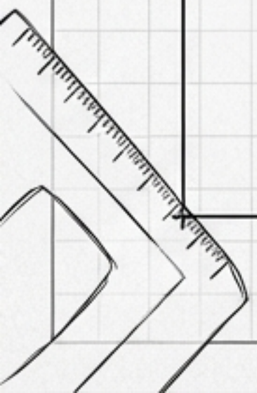
Networking

- [ ] Shared VPC Host/Service boundaries.
- [ ] Secure Tags vs legacy network tags.
- [ ] Premium vs Standard routing tiers.

IaC & Tooling

- [ ] gcloud storage vs legacy gsutil.
- [ ] Terraform remote state concepts.
- [ ] Config Connector vs Helm responsibilities.





// END OF ARCHITECTURAL BLUEPRINT.