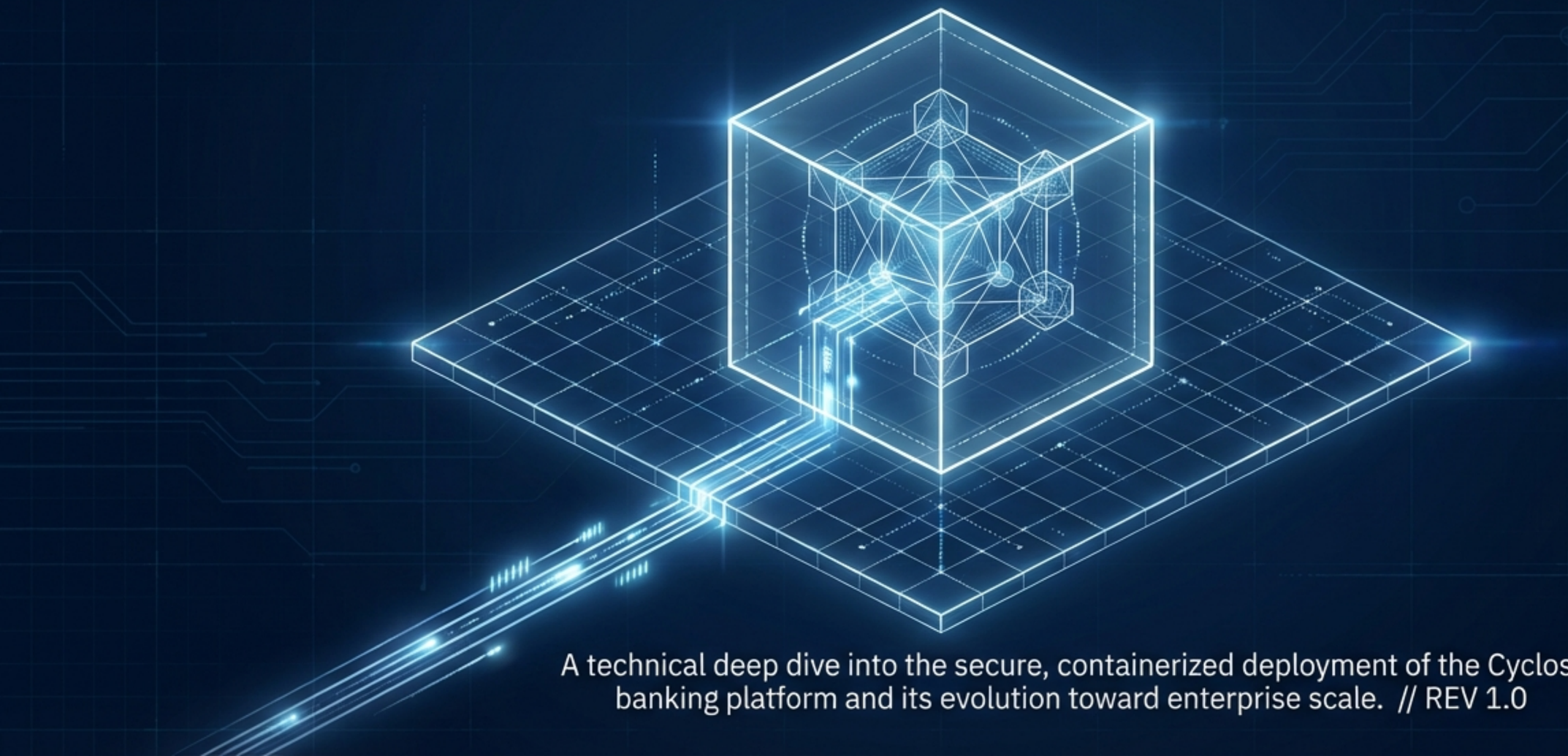
Cyclos on Google Cloud Platform

Architect Architecture & Strategic Roadmap



A technical deep dive into the secure, containerized deployment of the Cyclos banking platform and its evolution toward enterprise scale. // REV 1.0

Executive Summary: A Secure, Zero-Touch Foundation

The current deployment establishes a robust Base Configuration leveraging fully managed Google Cloud services.

Zero-Touch Initialization

Automated “init jobs” handle extension installation, user provisioning, and schema validation without manual intervention.

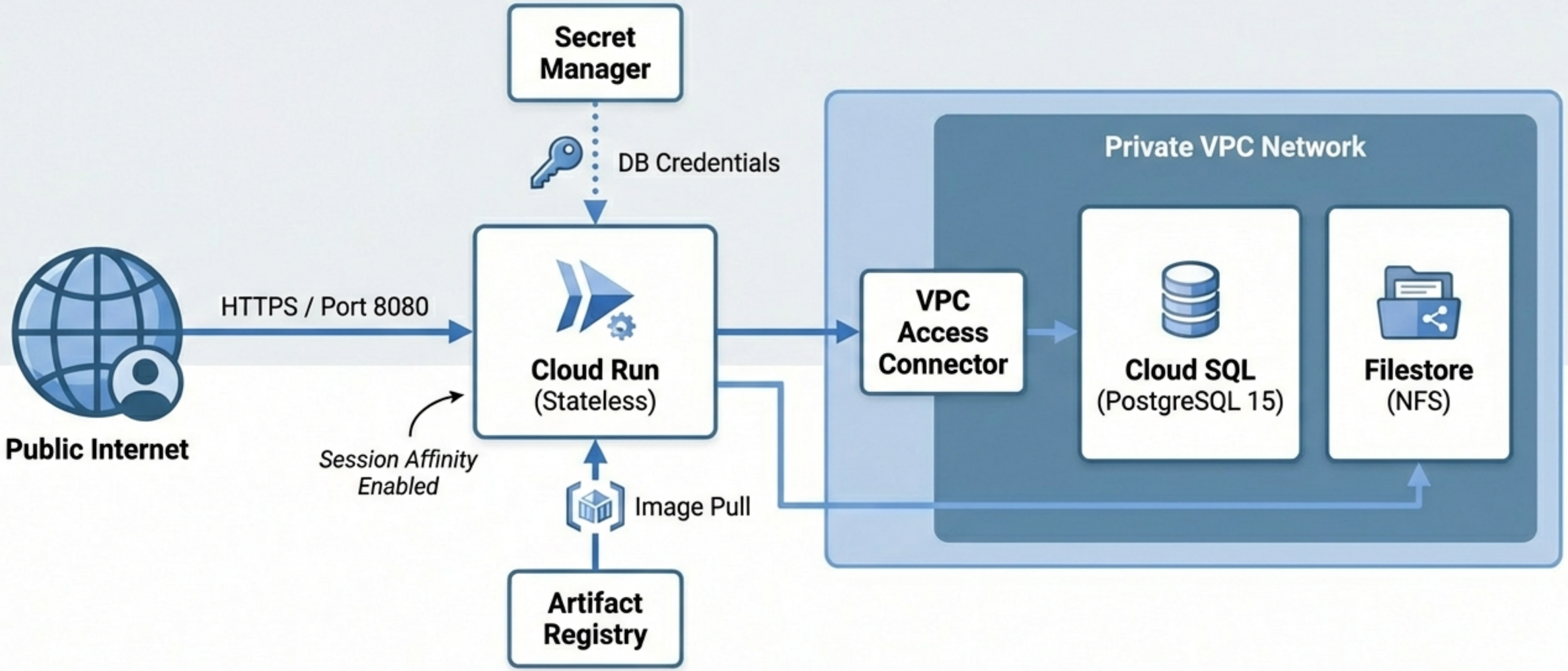
Least-Privilege Security

Runtime and deployment operations are strictly separated via distinct Service Accounts (cloud_run_sa vs. cloud_build_sa).

Private Connectivity

Internal traffic between application and database utilizes a Serverless VPC Access Connector. Data never traverses the public internet.

High-Level Architecture Map



Identity & Access Management: The Least-Privilege Model

Runtime Identity

`Service Account: cloud_run_sa`

- `roles/secretmanager.secretAccessor`
  (Access DB passwords)
- `roles/storage.objectAdmin`
  (App storage control)

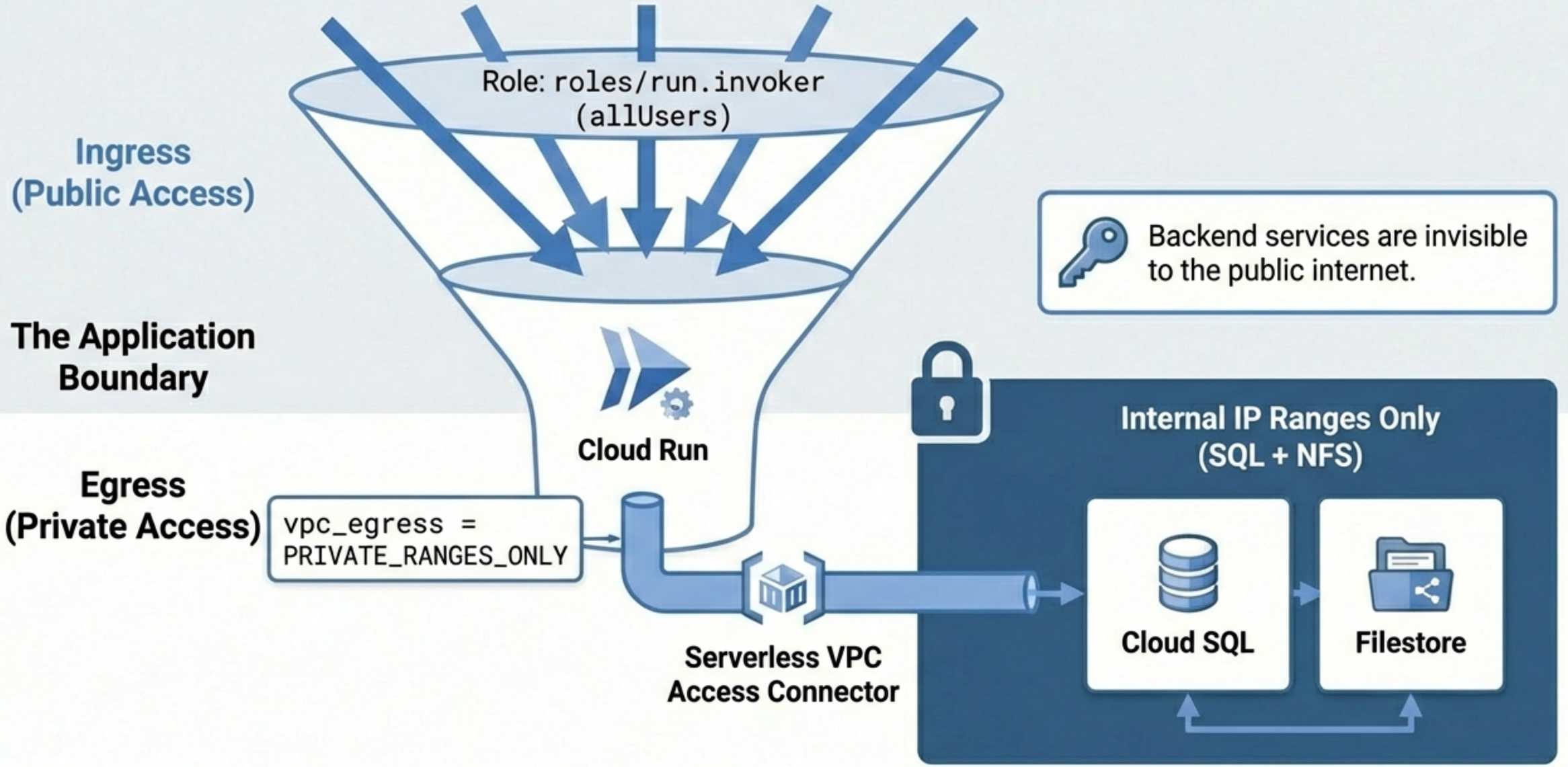
Deployment Identity

`Service Account: cloud_build_sa`

- `roles/run.developer`
  (Deploy revisions)
- `roles/iam.serviceAccountUser`
  (Impersonate runtime SA)

Secret Management: Database credentials (db_password) and API keys are stored in Google Secret Manager and injected at runtime. No hardcoded secrets.

Network Topology & Traffic Flow



Compute Configuration & Constraints

PLATFORM SPECS

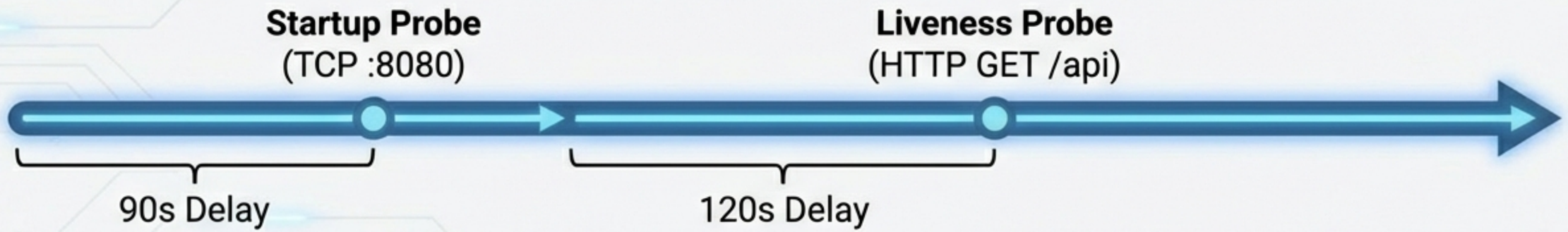
2 vCPU / 4GB Memory per instance

SCALING LIMITS

```
min_instance_count = 1
max_instance_count = 1
```

Auto-scaling disabled (Standalone Mode).
Session Affinity Enabled.

KUBERNETES PROBES



Data Persistence Layer

Managed Extensions (Dependency Order Enforced)

- `cube & earthdistance (Geospatial calculations)`
- `postgis (Advanced mapping data)`
- `pg_trgm (Text similarity search)`
- `uuid-ossp (UUID generation)`
- `unaccent (Accent-insensitive querying)`

Connectivity: PGSimpleDataSource via TCP

Application Logic: The ‘Standalone’ Profile

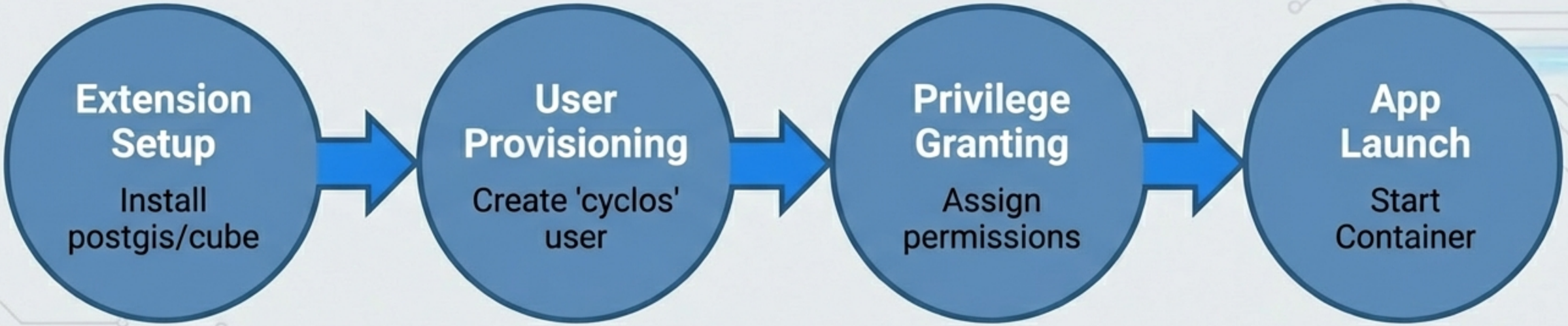
cyclos.properties

```
cyclos.db.managed = true                    // App handles DDL updates

# CURRENT CONSTRAINTS
cyclos.clusterHandler = none                // Isolated mode
cyclos.storedFileContentManager = db        // BLOB storage
cyclos.searchHandler = db                   // Search indexing on DB
```

Performance Bottlenecks to be addressed in Act II

Operational Automation & Provisioning

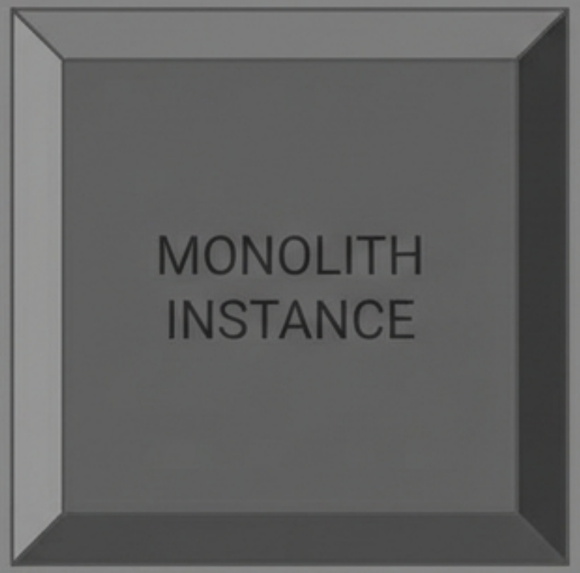


Credential Security

The 'cyclos' user authenticates via a high-entropy random password generated by Terraform. Immediately locked in Secret Manager.

Architecture Assessment: The Pivot to Scale

Current State: Secure Monolith



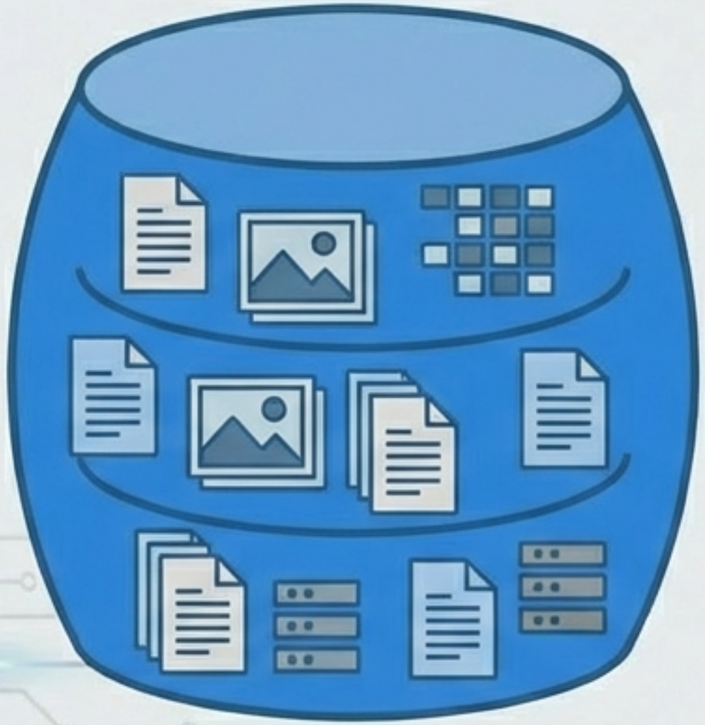
- Vertical Scaling Only
- Single Point of Failure (1 Instance)
- Low Operational Overhead

Strategic Enhancements

Target State: Distributed Scale

- Horizontal Scaling (N+1)
- Offloaded Compute (Search/Storage)
- High Availability Clustering

Enhancement A: Externalizing File Storage



Current: Files in DB

NFS Filestore (/mnt)

cyclos.storedFileContentManager = file

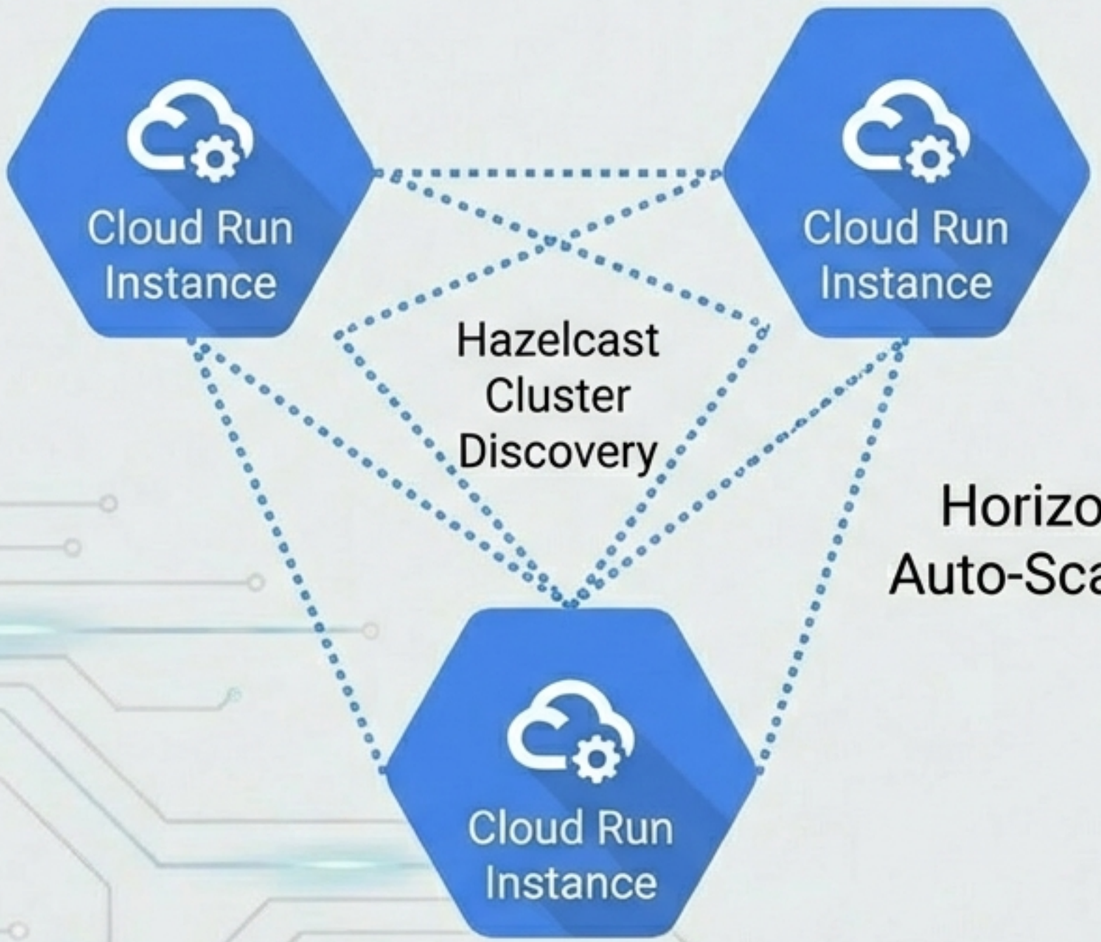
Google Cloud Storage

cyclos.storedFileContentManager = gcs

Reduces backup times, lowers database CPU load, enables infinite storage scale.

Enhancement B: Clustering & Auto-Scaling

Current: max_instance_count = 1



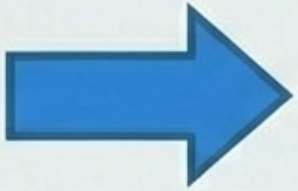
Horizontal Auto-Scaling

```
cyclos.clusterHandler = hazelcast
```

Shift compute to GKE or Multi-Instance Cloud Run

Enhancement C & D: Performance Offloading

Cloud SQL
Primary



OpenSearch Cluster

Externalize Search Indexing
cyclos.searchHandler = opensearch

Read Replicas

Offload Reporting Traffic
cyclos.datasource.readOnly.*

Enhancement E: IAM Database Authentication

Challenge: Eliminate static password rotation policies.

Solution: Authenticate directly using IAM identity tokens.

Benefit: Rotation-free, identity-based security.

The Evolution Roadmap

Foundation
(Status: Complete)

- [x] Containerized on Cloud Run
- [x] Private VPC Networking
- [x] Automated Schema & User Init

Optimization
(Next Steps)

- [ ] Offload File Storage (NFS/GCS)
- [ ] Externalize Search (OpenSearch)
- [ ] Implement IAM DB Auth

Scale
(Enterprise Goal)

- [ ] Enable Hazelcast Clustering
- [ ] Activate Auto-Scaling
- [ ] Deploy Read Replicas