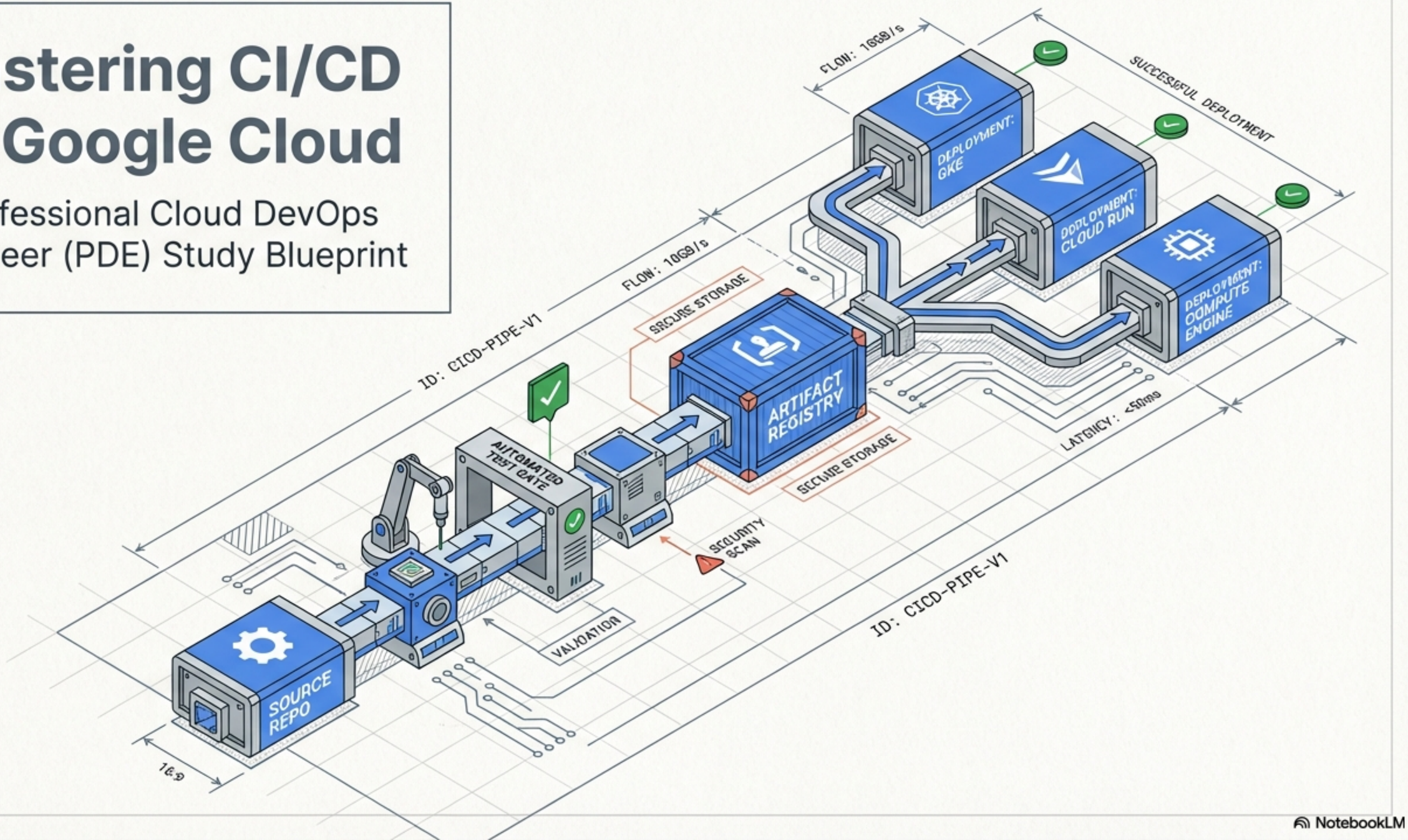
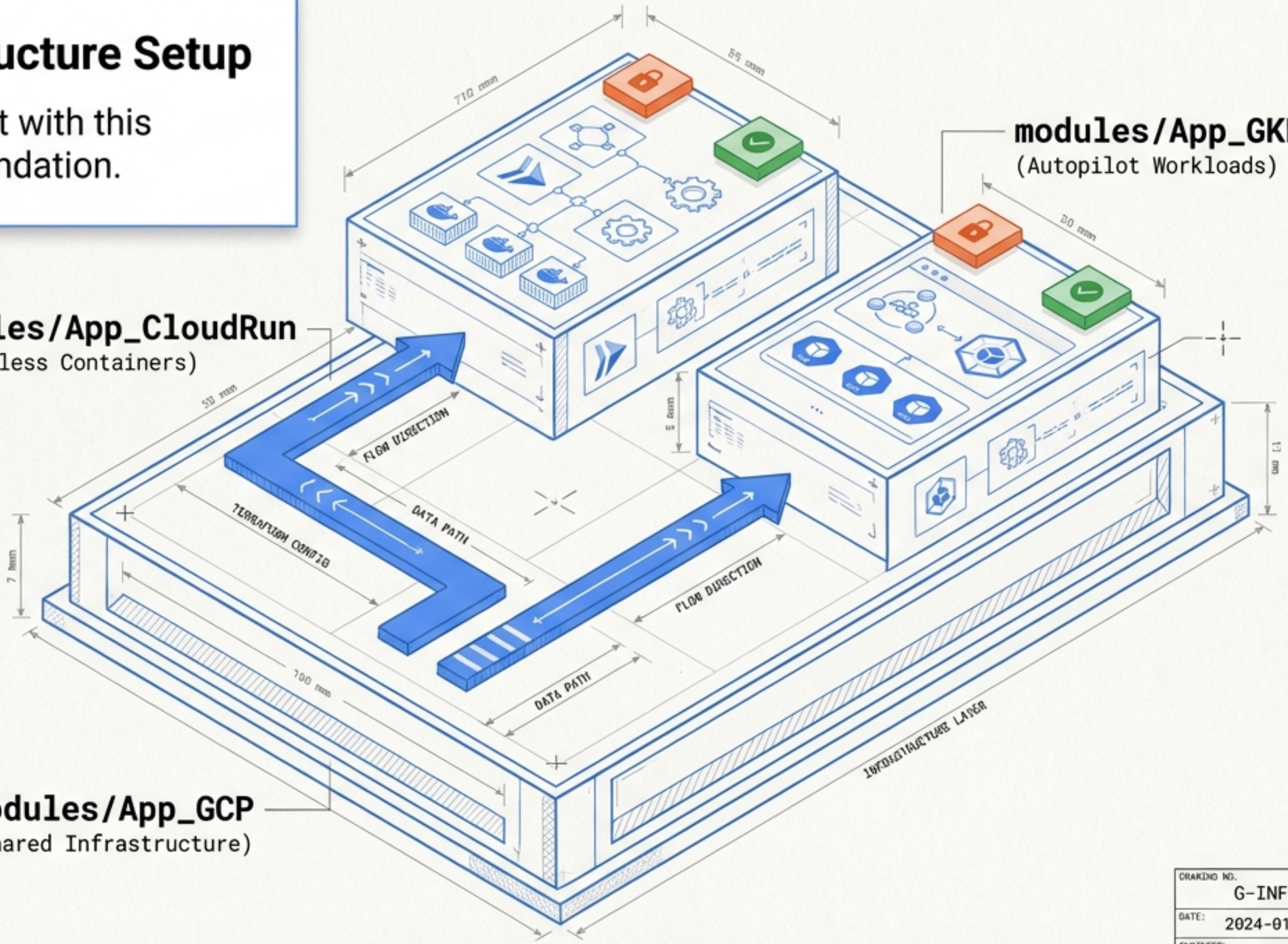
Mastering CI/CD on Google Cloud

A Professional Cloud DevOps Engineer (PDE) Study Blueprint



The Core Infrastructure Setup

All CI/CD flows interact with this specific Terraform foundation.



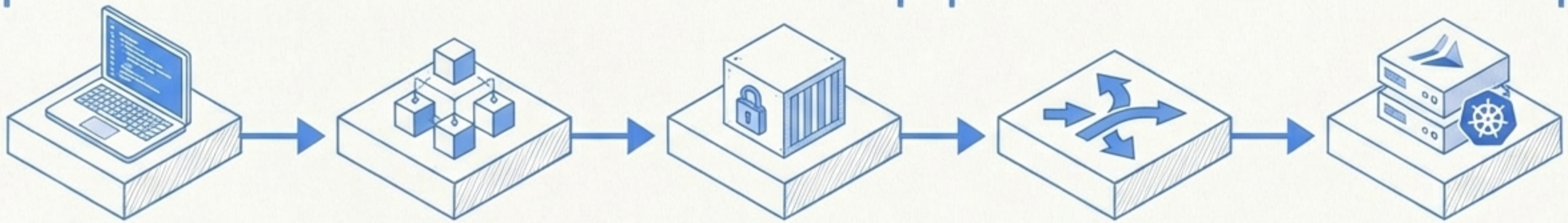
DRAWING NO.	G-INFRA-001
DATE:	2024-01-15
ENGINEER	ARCHITECT T.
REV:	A

The End-to-End CI/CD Journey

Domain 2.3: Configuration & Secrets

Domain 2.1: Designing Pipelines

Domain 2.2: Managing Deployments



Source Code Push

Cloud Build

Artifact Registry

Cloud Deploy

Cloud Run / GKE

Domain 2.4: Auditing & Logging

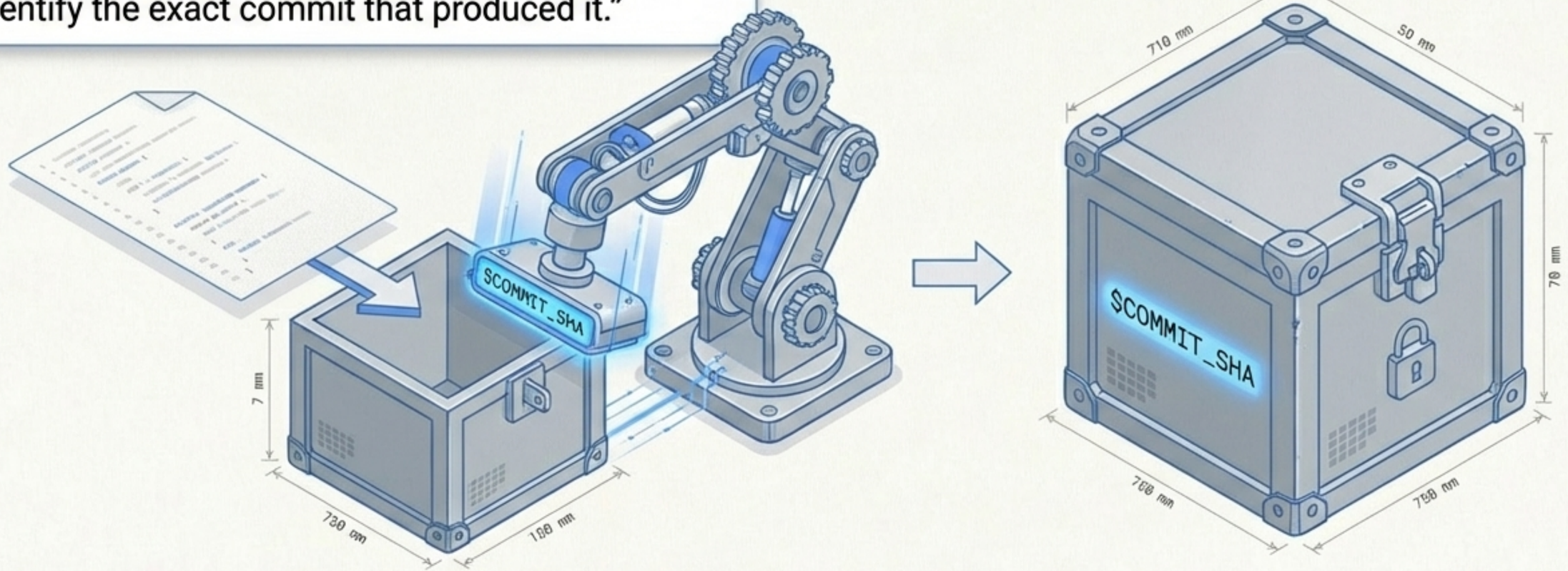
DRAWING NO. G-INFRA-001

DATE: 2024-01-15

ENGINEER: ARCHITECT

The Immutable Artifact

> “Given any running container, you must be able to identify the exact commit that produced it.”

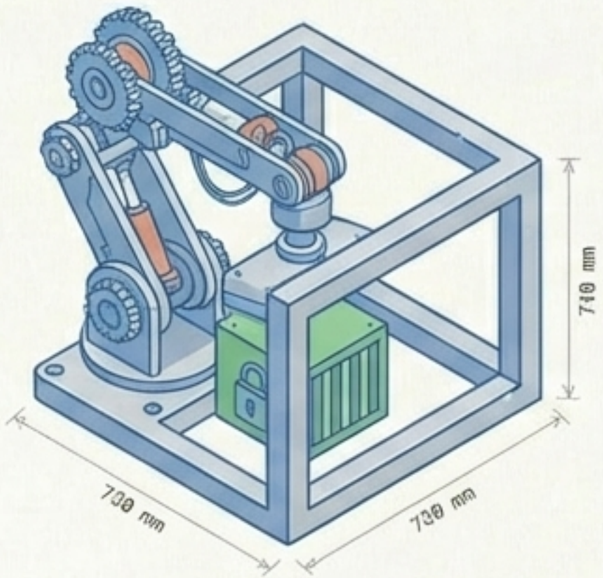



```
.../${_REPO_NAME}/${_IMAGE_NAME}:${COMMIT_SHA}
```

DRAWING NO. G-INFRA-002
DATE: 2024-01-15
ENGINEER: ARCHITECT

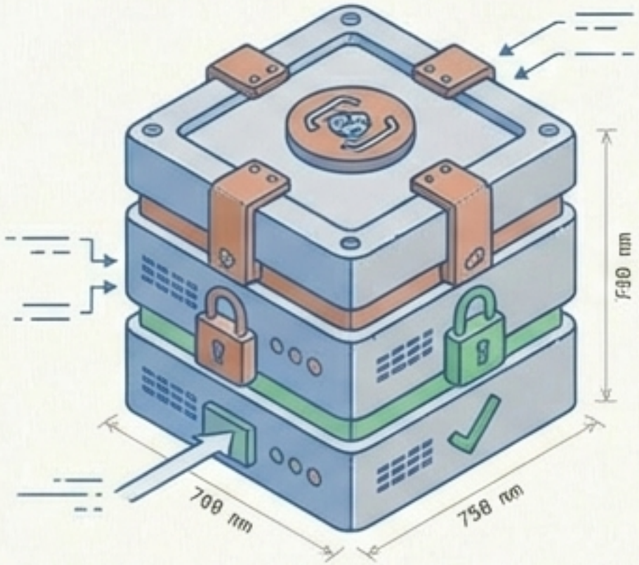
Domain 2.1: Designing Pipelines

Secure Builds with Kaniko



Daemonless execution. Builds entirely inside a `standard container` without requiring `privileged` mode. Safer than Docker-in-Docker.

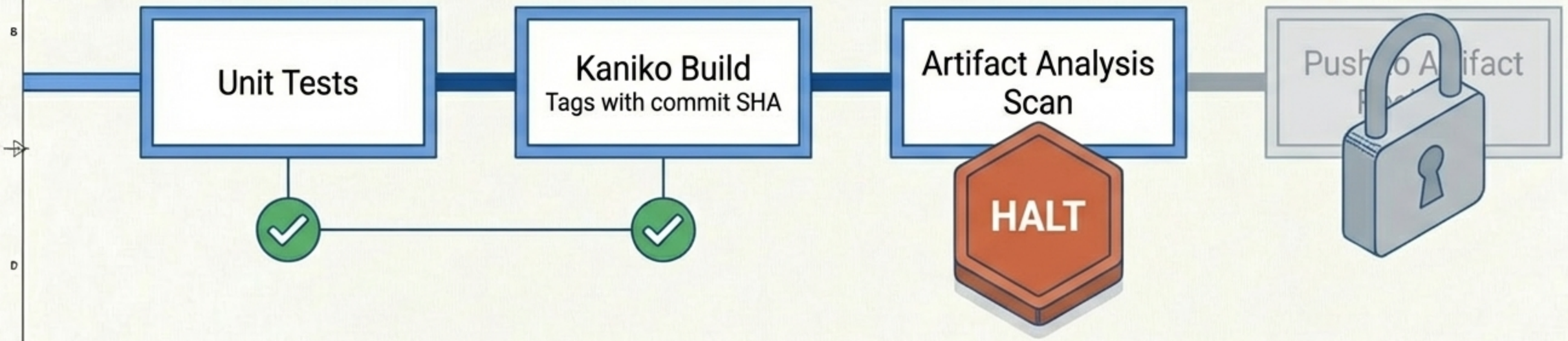
Artifact Registry & Analysis



Regional storage and multi-format support. Automatically scans pushed images for known CVEs via integrated `Artifact Analysis`.

DRAWING NO.	G-INFRA-002
DATE:	2024-01-15
DESIGNED BY:	ARCHITECT

Real-World Scenario: The Gaming Platform



Pipeline halts automatically with a non-zero exit code if a CRITICAL CVE is detected. Cloud Monitoring alerts catch zero-day vulnerabilities in already-deployed versions.

G-INFRA-002

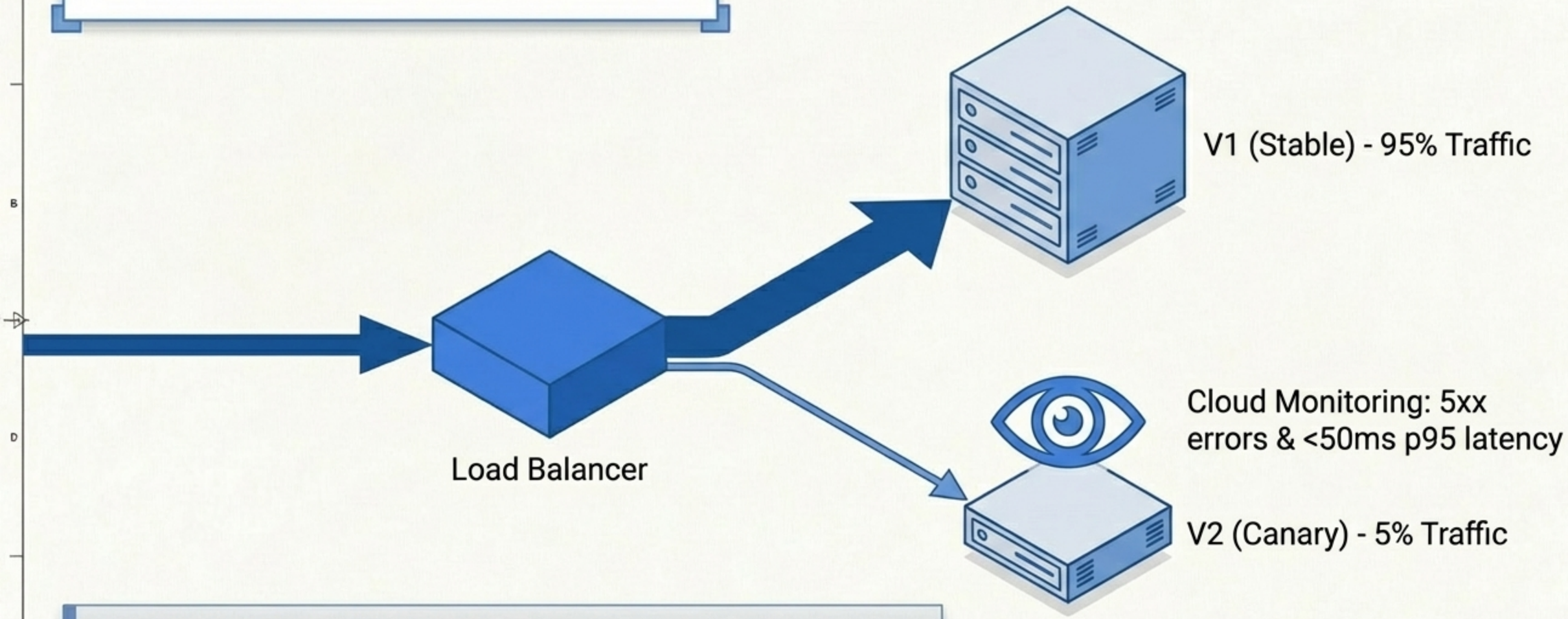
2024-01-15

Deployment Strategies Comparison

Strategy	GCP Service	Mechanism	Rollback Speed
Canary Deployments	`Cloud Run`	Native traffic splitting (e.g., 5% vs 95%)	Instant
Staged Rollouts	`Cloud Deploy`	Delivery pipelines (Dev -> Staging -> Prod) with promotion gates	Fast (Retains previous release)
Instant Rollbacks	`Cloud Run & Deploy`	Redirect traffic back to previous revision without rebuilding	< 10 Seconds

DRAWING NO: G-INFRA-003
DATE: 2024-01-15
REV: A
CHECKED BY: ARCHITECT_T

Anatomy of a Canary Rollout



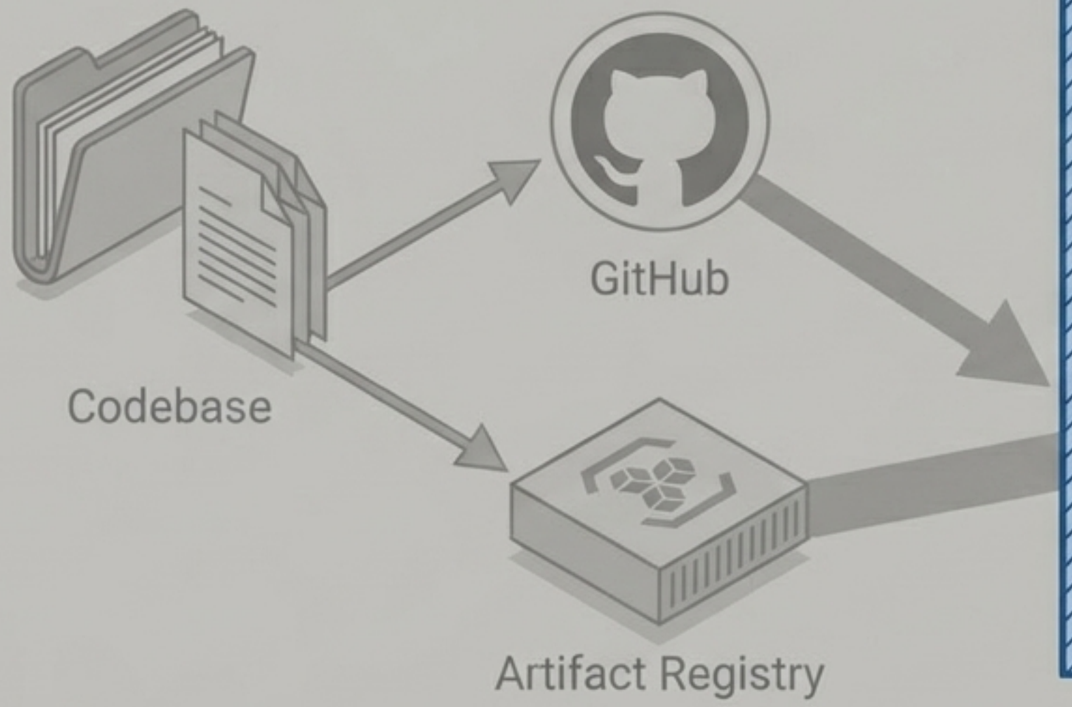

```
traffic_split { percent = 5 revision_name = "v2-canary" }
traffic_split { percent = 95 revision_name = "v1-stable" }
```

G-INFRA-002

2024-01-15

The Zero-Plaintext Principle

The container image never contains the secret. It is resolved strictly at runtime into container memory, bypassing disk entirely.



Secret Manager

Cloud Run Container

secret_environment_variables

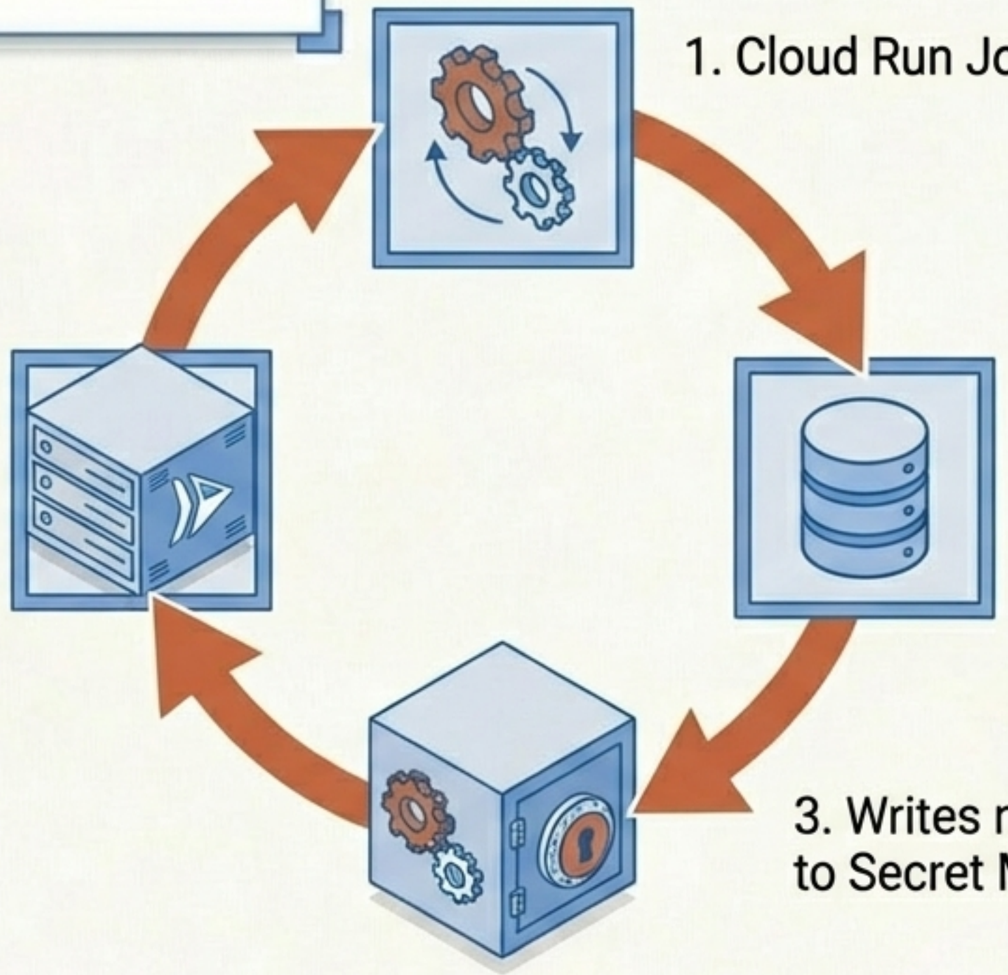
secret_environment_variables

Cloud Run Container

```
value_source { secret_key_ref }
```

	DRAWING NO: G-INFRA-003	
	DATE: 2824-01-15	REV: A
	CHECKED BY: ARCHITECT_T	

Automated Credential Rotation



1. Cloud Run Job executes

2. Generates and updates password in Cloud SQL

3. Writes new version directly to Secret Manager

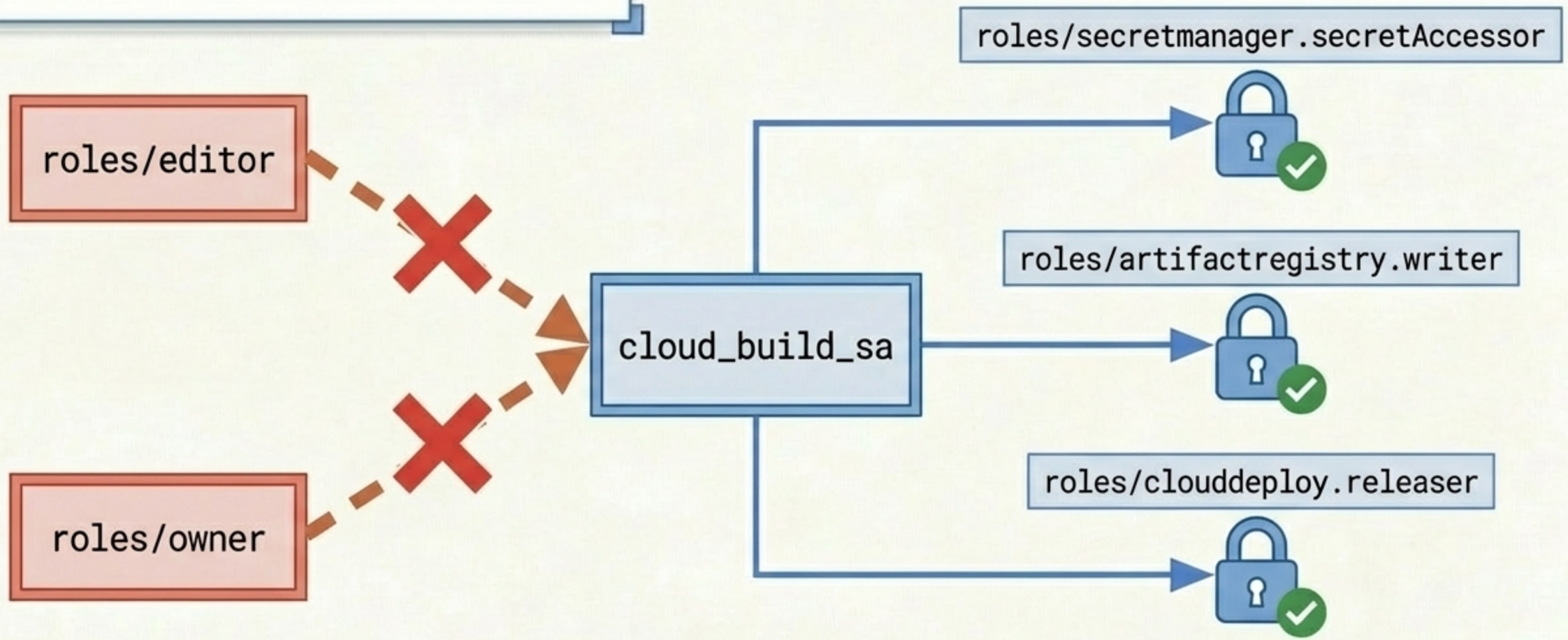
4. Cloud Run automatically picks up new version on the next revision deployment

Zero human intervention. No code changes. No manual credential updates.
If rotation fails, Cloud Monitoring fires an alert immediately.

G-INFRA-002

2024-01-15

Principle of Least Privilege



Source repository connections use Google-managed OAuth tokens—no raw repository access tokens need to be stored in Secret Manager.

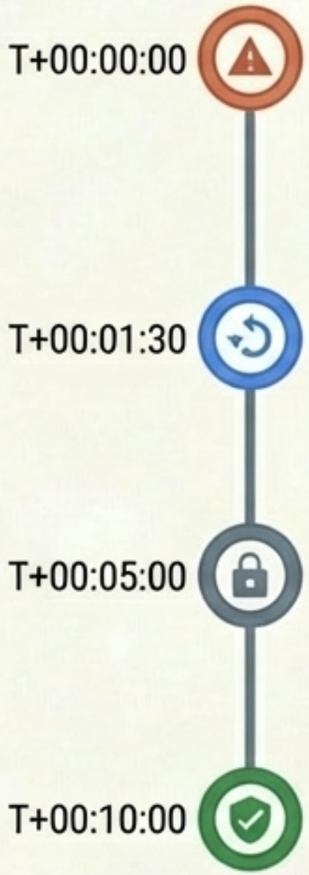
G-INFRA-003

2024-01-15

The Tamper-Proof Audit Trail

What you want to know	Where to look	Evidence
Was the build tampered with?	Artifact Registry 	`SLSA Provenance` (Cryptographically signed record of inputs/outputs)
Who approved this production deployment?	Cloud Deploy 	`Release History` (Stages, timestamps, user approvals)
What changed in the infrastructure?	Cloud Storage 	`Terraform State` (Object versioning provides a chronological snapshot history)

Real-World Scenario: The Unauthorized Deployment



1. Detection

Cloud Audit Logs flag a `ReplaceService` event from a direct `gcloud run deploy` command (developer bypasses pipeline).

2. Rollback

Cloud Deploy instantly triggers a redeploy of the last known-good release.

3. Lockdown

IAM privileges updated to remove `roles/run.developer` from individual accounts.

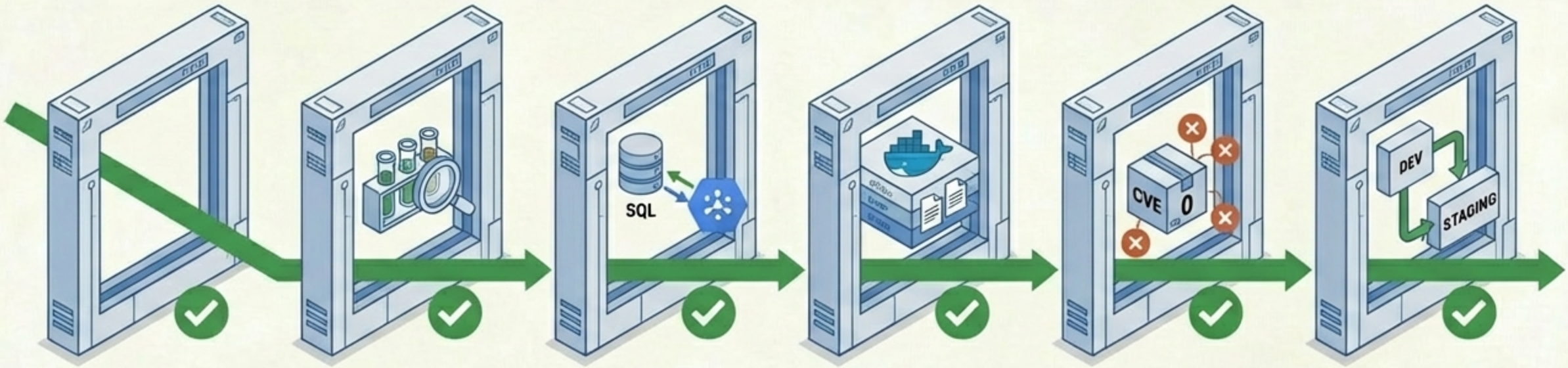
4. Enforcement

Binary Authorization enabled to block any future image lacking a valid Cloud Build attestation.

G-INFRA-004

2024-01-15

Quality Gates & Automation. The Unbreakable Chain.



git

Unit Tests
Fast execution

Integration Tests
Live Cloud SQL/PubSub

Container Structure Tests
Verify expected files/envs

Artifact Analysis
CVE blocks

Automation Rules
Auto-promote Dev -> Staging

G-INFRA.004

2024-01-15

The PDE CI/CD Checklist

Designing (Domain 2.1)

Focus: Immutable Artifacts
Key Services: Kaniko, Artifact Registry, Artifact Analysis
Metric: `$COMMIT_SHA`

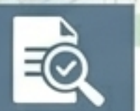
Managing (Domain 2.2)

Focus: Progressive Rollouts
Key Services: Cloud Deploy, Cloud Run Traffic Splitting
Metric: Canary & Rollbacks

Secrets (Domain 2.3)

Focus: Zero-Plaintext
Key Services: Secret Manager, Cloud Run Jobs (Rotation)
Metric: `Runtime Injection`

Auditing (Domain 2.4)



Focus: Tamper-Proofing
Key Services: Cloud Audit Logs, SLSA Provenance, GCS Object Versioning
Metric: Diagnostic Forensics