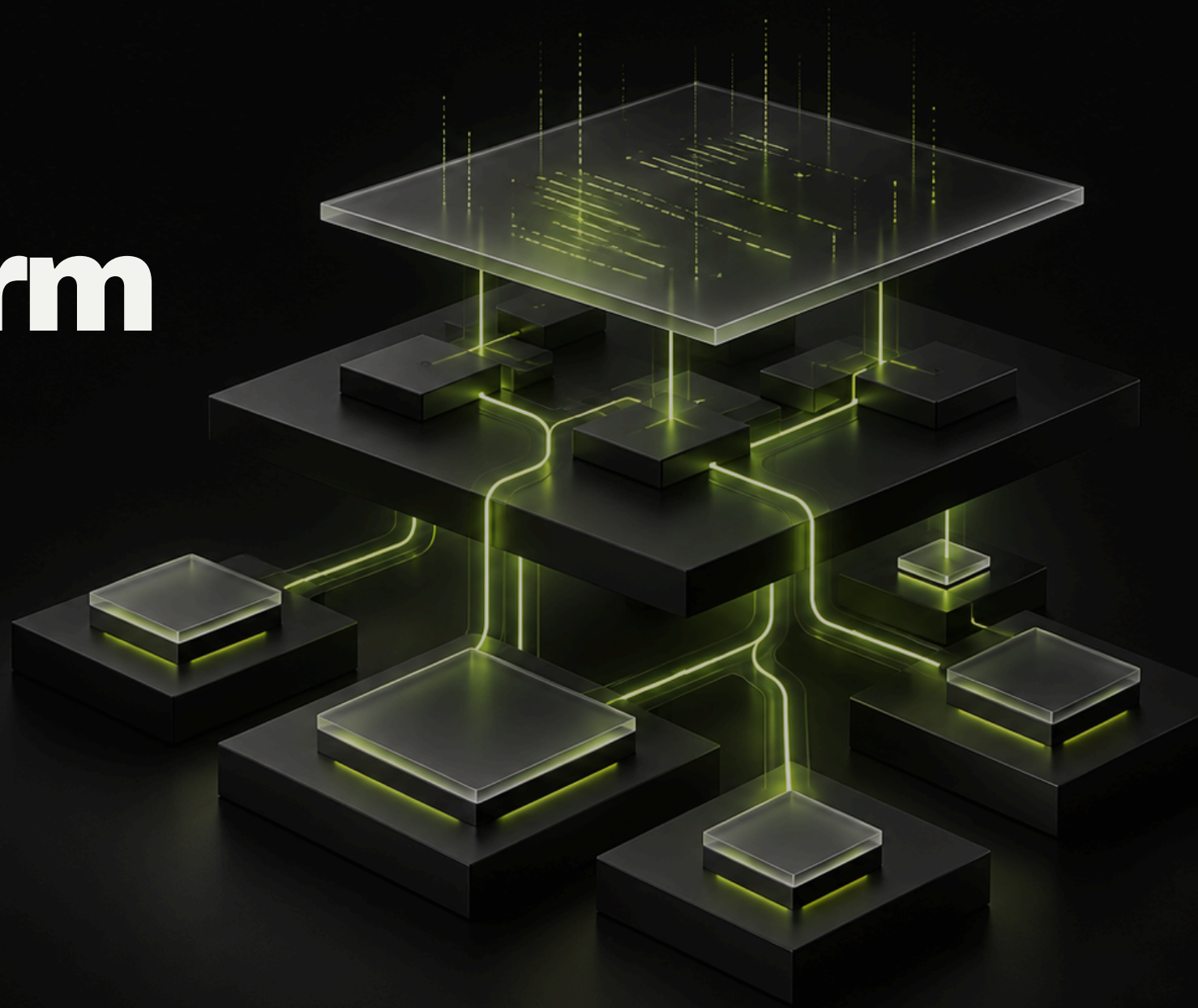


GOLF / GOLF ON CLOUDFLARE

A Git platform built on Cloudflare.

A native Git workflow across the Cloudflare platform.



From source to software.

Golf connects Git, collaboration, executable evidence, optional proposals and protected previews.

01

Source

Repositories, history, issues, PRs and human review.

02

Evidence

Approved exact-source tests, reports and proposals.

03

Delivery

Protected static and bounded Worker app previews.

Docker: the portable Golf stack.

Run a complete developer core on your machine or owned Docker infrastructure.

01

What runs

Golf React/Go, Forgejo and independent PostgreSQL databases/roles. Private configuration and persistent volumes survive ordinary restarts.

02

How to start

Initialize private environment files, start Compose, check /readyz, then enroll a mapped Golf account. Optional Docker workers, agents and object storage require their own setup.

03

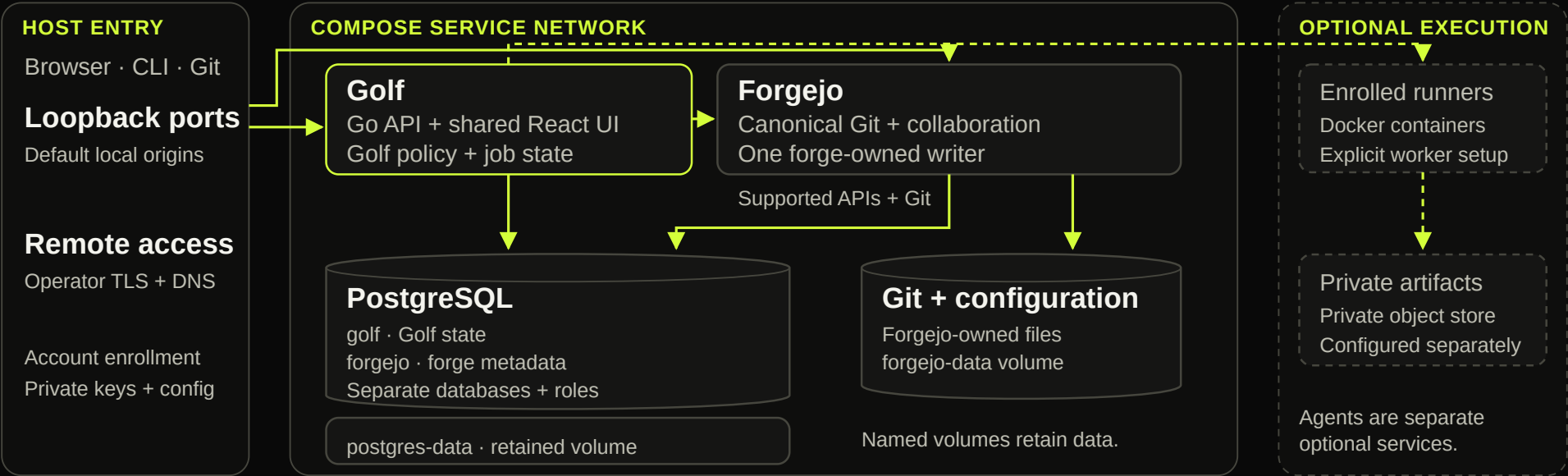
What you own

Image/version choices, HTTPS beyond loopback, secrets, data volumes and coordinated recovery. No Cloudflare or AI account is needed for core work.

Docker: what runs, what persists.

The portable core uses Forgejo and PostgreSQL. Execution workers are allocated separately.

g golf. DOCKER / PORTABLE SERVICE OWNERSHIP



Golf uses forge APIs; each service owns its data. Persistence and recovery need operator verification.

[Editable architecture diagram](#) · [Open full size](#)

Kubernetes: deploy Golf deliberately.

Golf's Helm chart packages the portable core and makes its operating boundaries explicit.

01

What the chart supplies

Golf replicas, one Forgejo writer, optional PostgreSQL, resources/probes, retained claims, non-root isolation and default-deny policies.

02

How it is hardened

Upgrade identity/endpoint fences, API hostname spread and multi-replica disruption budget, graceful drain, private database CA mounts and explicit DNS/egress peers.

03

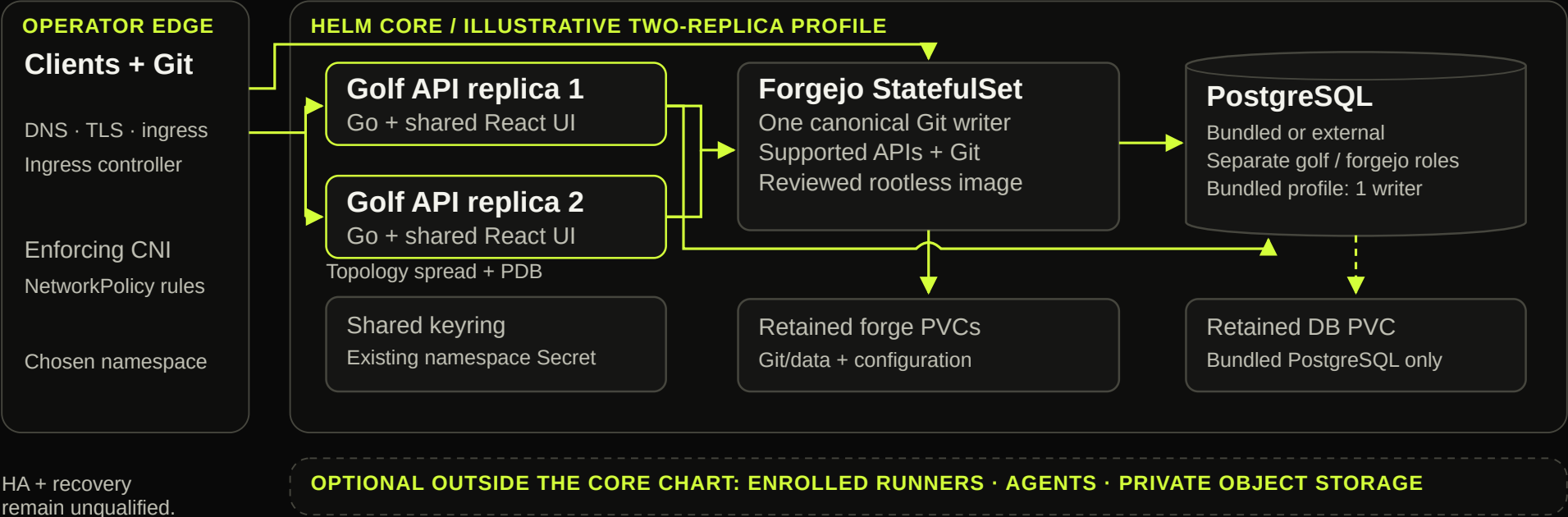
What you supply

Built image, existing credential/certificate Secrets, enforcing CNI, storage, ingress/TLS/DNS and a tested recovery procedure. Runners and agent services remain separate.

Kubernetes: placement and ownership.

API replicas share one forge writer and retained storage. More replicas alone do not establish HA.

g golf. KUBERNETES / REPLICAS AND RETAINED DATA



[Editable architecture diagram](#) · [Open full size](#)

Cloudflare: a native hosted control plane.

Artifacts, D1 and Workers replace origin-backed forge infrastructure on this track.

01

What runs

Shared UI/Connect services in Workers; Artifacts canonical Git; D1 collaboration/policy; SQLite Durable Objects coordinating reads and execution.

02

How the workflow grows

Queues, Workflows and Containers produce evidence. Private R2, managed registry and protected Worker apps retain outputs. Optional AI, browser snapshots, email and operations add focused consumers.

03

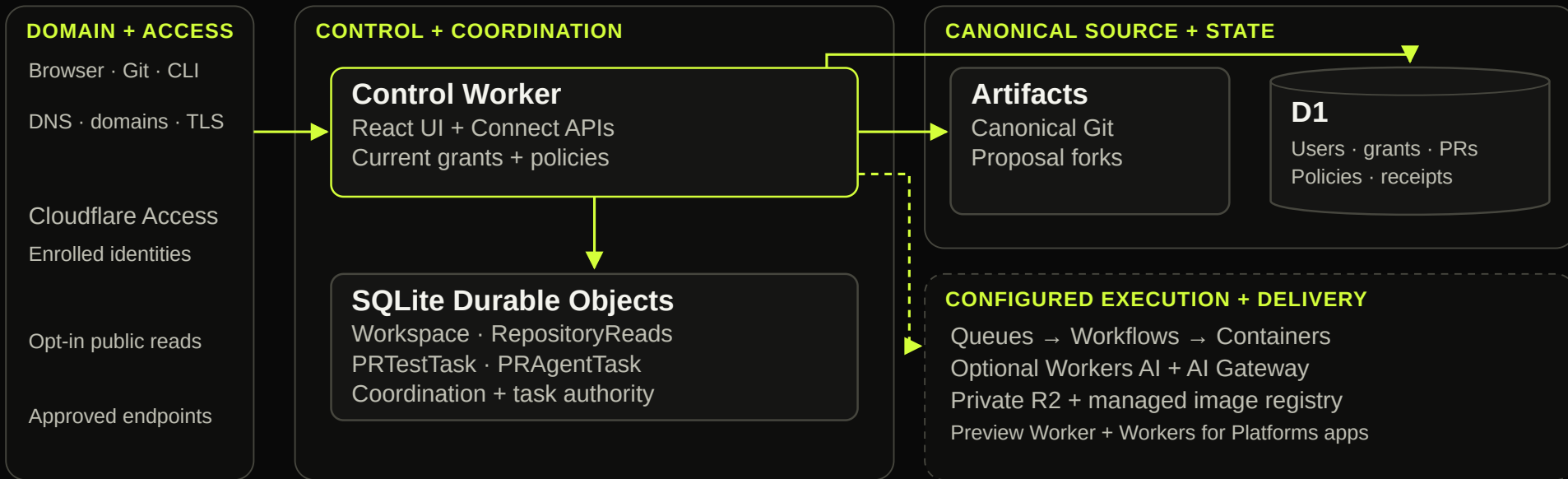
How to deploy

Alchemy or the native cf recipe provisions owned resources under the selected account, Access identity, domains, images and permissions. Verify actual schema, grants, readback and cleanup.

Cloudflare: where each part lives.

Workers own the application, Artifacts owns Git, and D1 owns collaboration state.

CLOUDFLARE / NATIVE OWNERSHIP AND PLACEMENT

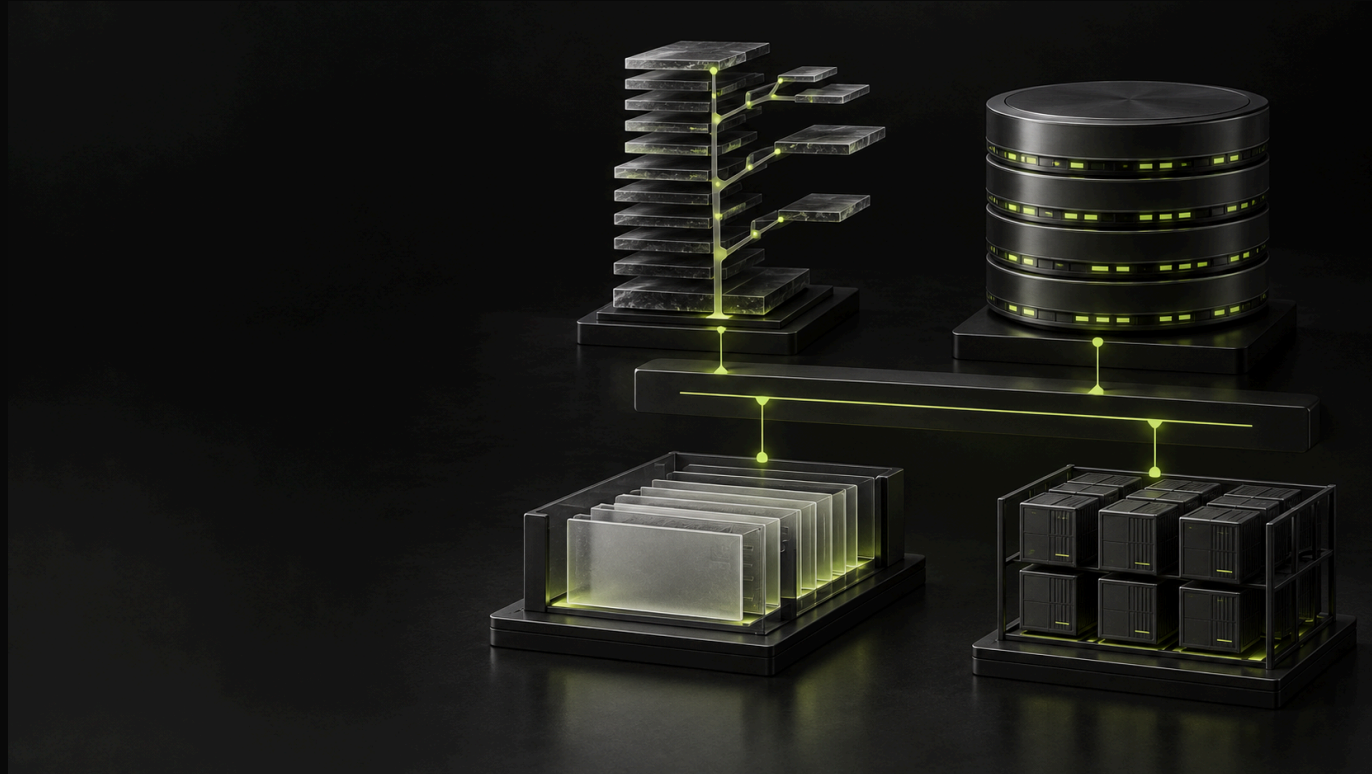


Configured services, current permissions and execution evidence determine available workflows.

[Editable architecture diagram](#) · [Open full size](#)

The storage roles have different jobs.

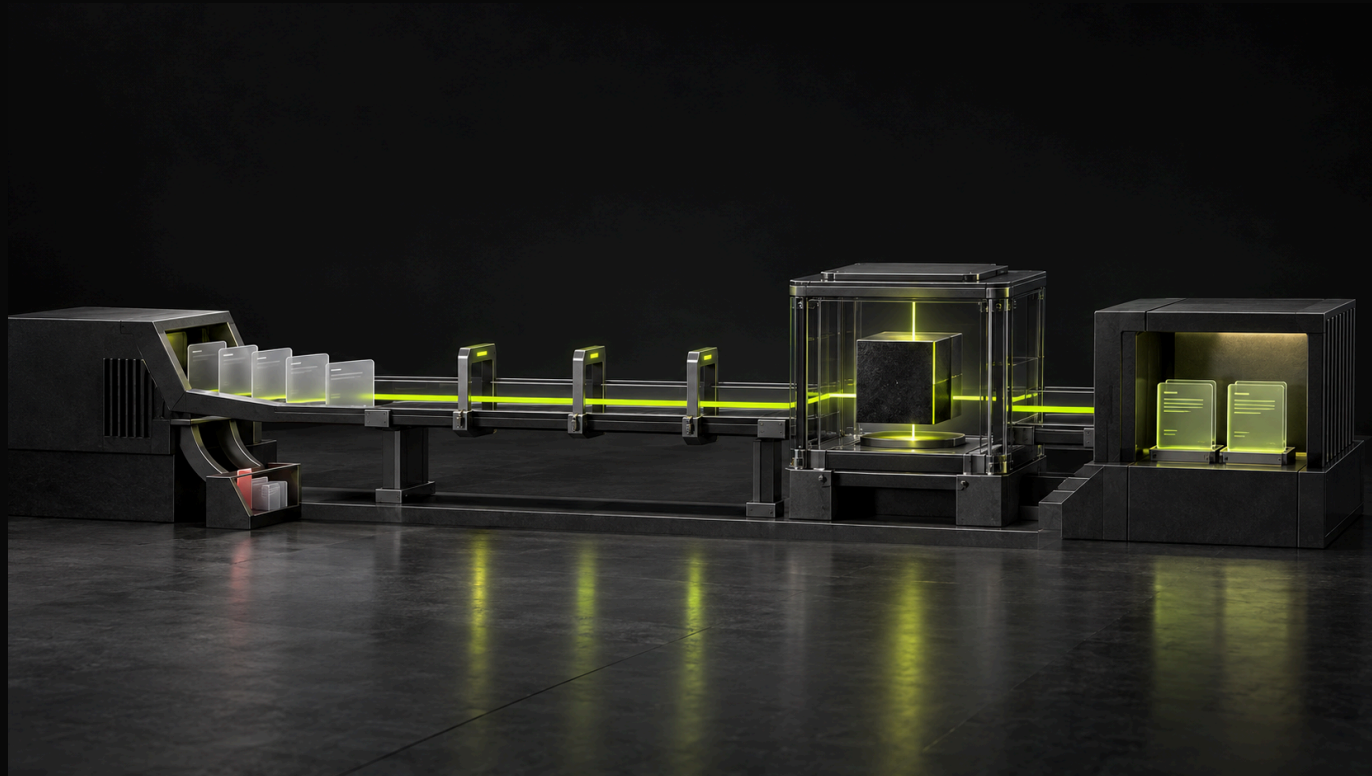
Artifacts keeps Git; D1 keeps domain state; private R2 keeps outputs; the managed registry keeps images.



Conceptual illustration · exact services on adjacent slides · [Open full size](#)

A durable path to executable evidence.

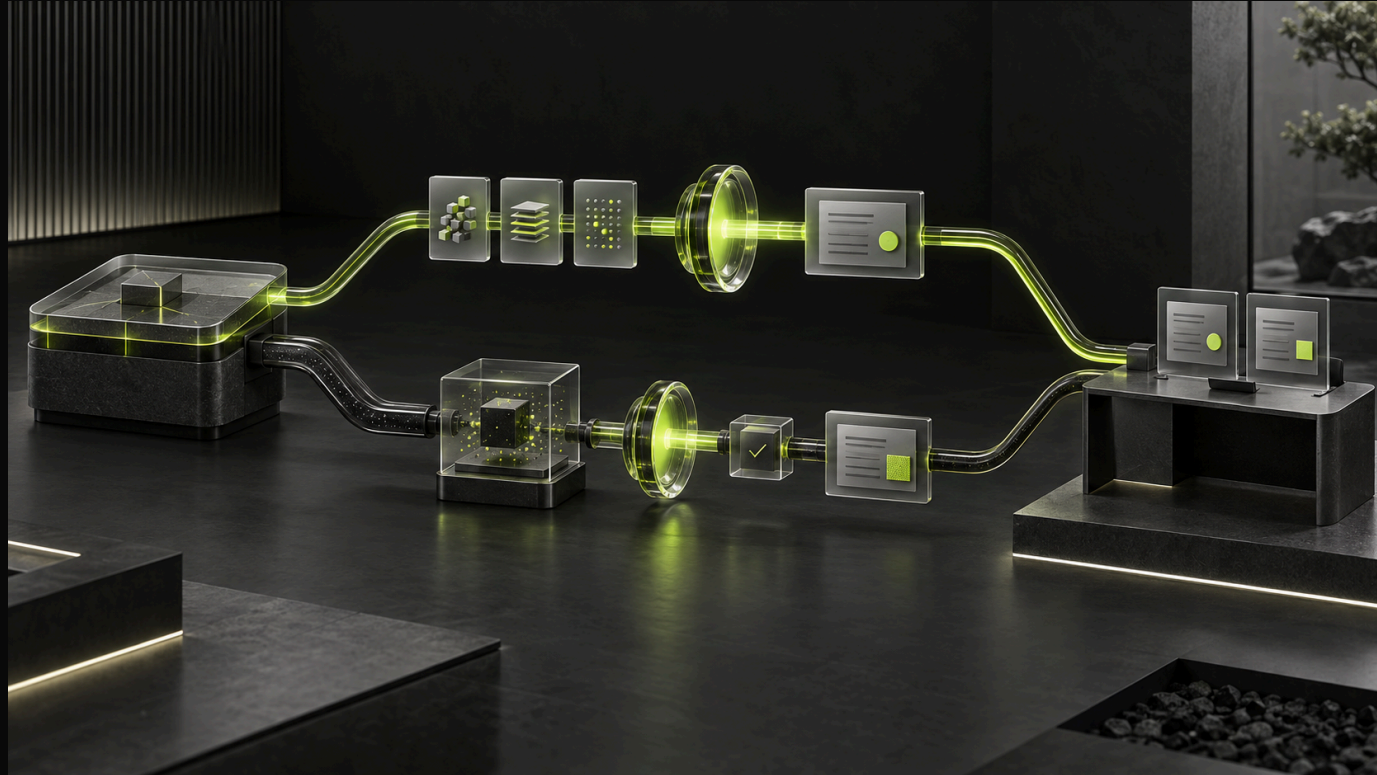
Authorized exact-source work passes from intake through orchestration and approved compute to private reports.



Conceptual illustration · exact services on adjacent slides · [Open full size](#) ↗

Advice and proposals are separate paths.

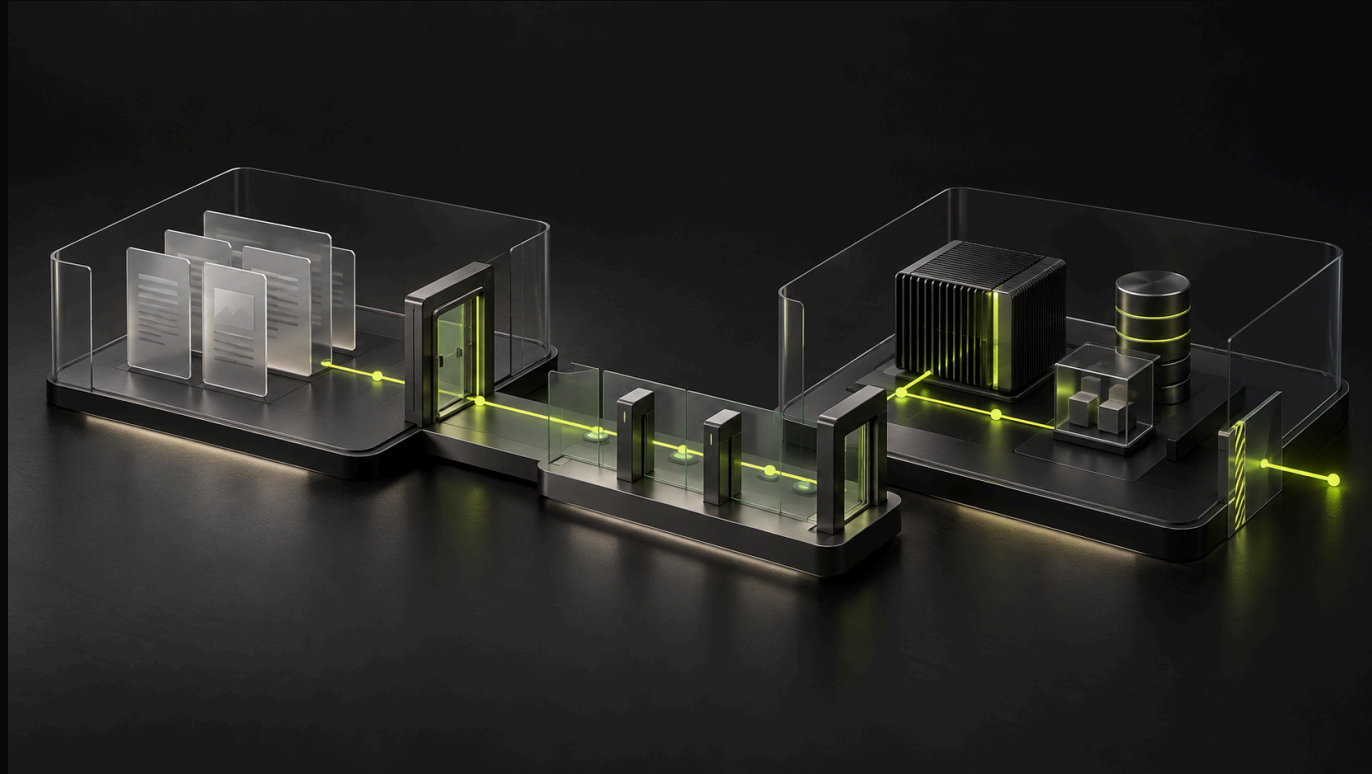
Clef sees metadata. Executable proposals work on an independent fork and return tests and a patch for human review.



Conceptual illustration · exact services on adjacent slides · [Open full size](#) ↗

A running preview has its own boundary.

Static bundles and Worker applications stay protected, isolated and subject to current reader/lease checks.



Conceptual illustration · exact services on adjacent slides · [Open full size](#) ↗

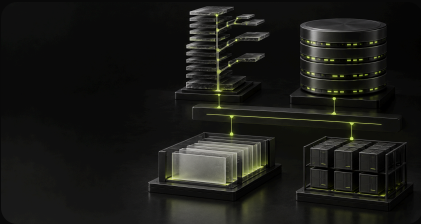
Workers

The product entrypoint

ROLE IN GOLF

Purpose in Golf

Serves the shared Golf UI, native APIs, Git brokerage and trusted service entrypoints at custom domains. UI files are embedded in the control Worker.



How the workflow uses it

A browser, Git client or Golf CLI reaches the control Worker. Generated Connect handlers and broker entrypoints enforce the same current Golf authority.

Current operating boundary

Full native forge parity, fleet scale and SaaS onboarding remain open.



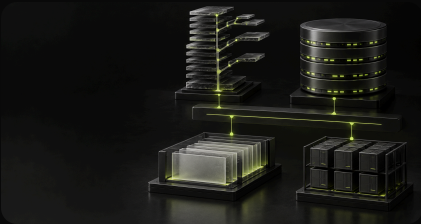
Artifacts

Canonical source and proposal isolation

ROLE IN GOLF

Purpose in Golf

Stores canonical Git objects/refs and independent agent forks; supports clone/push, source/history/diffs and first-slice standard PR merge.

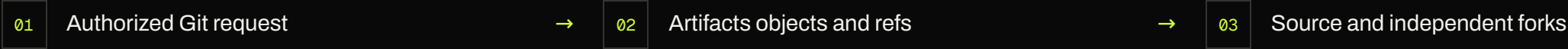


How the workflow uses it

A private Git push/clone goes through Golf admission and short-lived brokered provider access. An agent receives a separate fork; source/history/diffs stay bound to exact objects.

Current operating boundary

Merge requires same repository and base ancestor of head; no tree merge, squash, protected merge or native repository deletion.



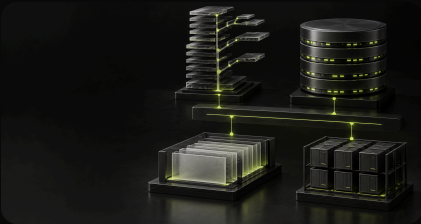
D1

Collaboration with current permission

ROLE IN GOLF

Purpose in Golf

Stores identities, grants, collaboration, operation journals, evidence intake, environments, email outbox and encrypted execution values; separate D1 databases back Worker previews.

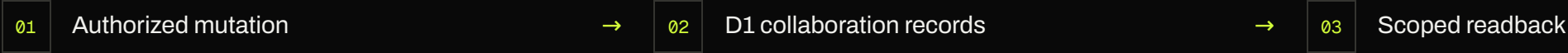


How the workflow uses it

An issue, PR, review, environment policy or execution intent becomes a versioned domain record. Users/grants, outboxes and readback receipts remain Golf-owned SQL state.

Current operating boundary

Recovery, broader authorization matrices and complete repository parity remain open.



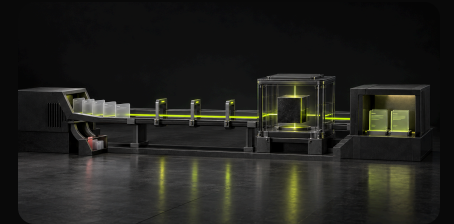
Durable Objects

Different objects, different responsibilities

ROLE IN GOLF

Purpose in Golf

SQLite workspace authority serializes writes/revocations, admits bounded concurrent reads and coordinates tasks; read shards scale immutable-source reads; alarms run maintenance when Cron stops arriving.

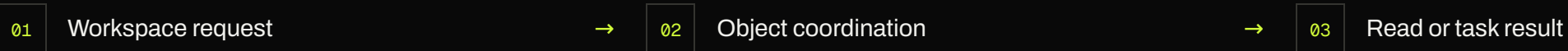


How the workflow uses it

Workspace coordinates authority/journals and maintenance.
RepositoryReads serves bounded reads; PRTestTask and PRAgentTask own the approved test/proposal compute lifecycle.

Current operating boundary

Bounded single-installation qualification, not global scale or provider availability.



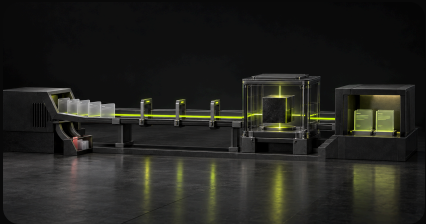
Containers

Run the approved profile

ROLE IN GOLF

Purpose in Golf

Runs exact-source approved CI and OpenCode proposals in DO-managed Linux containers with outbound interception and verified destruction.

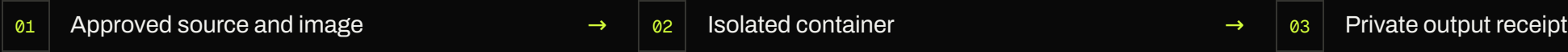


How the workflow uses it

Capture exact source and execute one approved Actions workflow or Python module in the reviewed image. Keep terminal status, denied requests and private output; do not infer general workflow compatibility.

Current operating boundary

One approved Actions path or Python module; Internet denied; arbitrary upstream workflows and hostile-repo isolation not qualified.



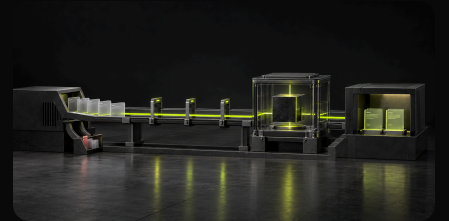
Sandbox SDK files

Stage files inside Containers

ROLE IN GOLF

Purpose in Golf

Uses @cloudflare/sandbox Files and SandboxFileError to access container files alongside raw ctx.container execution.

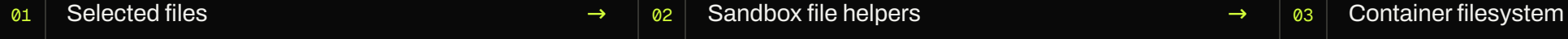


How the workflow uses it

The harness uses Sandbox SDK helpers to stage and read files inside raw Containers.

Current operating boundary

Golf uses raw ctx.container execution. It does not instantiate getSandbox or a Sandbox class.



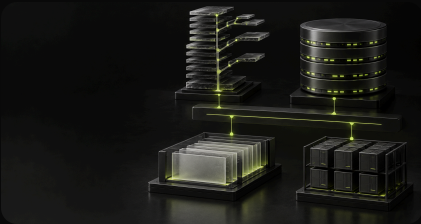
Managed image registry

Bind an image to the job

ROLE IN GOLF

Purpose in Golf

registry.cloudflare.com holds pinned runner images and digest-verified per-job OCI artifacts; trusted Worker brokers short-lived account registry credentials.

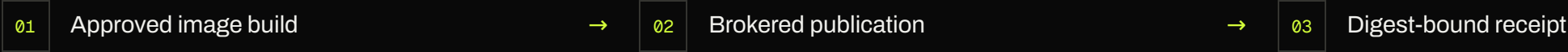


How the workflow uses it

The approved execution image is published to registry.cloudflare.com. Authorized CI publication and image inventory retain exact digests and repository/job receipts; provider authority stays inside the broker.

Current operating boundary

Golf brokers provider authority and preserves repository/job approval. Broader image scanning, trust and retention policy remain separate acceptance.



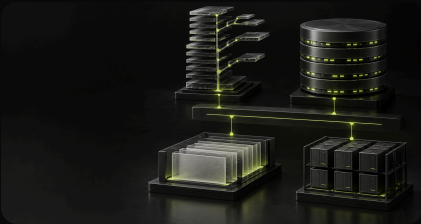
R2

Private objects with source identity

ROLE IN GOLF

Purpose in Golf

Private immutable reports, context/results, read indexes, static previews, screenshots, per-preview app files, release assets and discussion attachments.

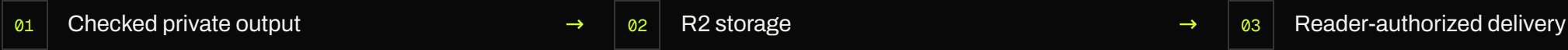


How the workflow uses it

Reports, context, patches and preview bundles are retrieved only with current reader authority. Bounded release assets and discussion uploads retain original receipts and verified download digests.

Current operating boundary

Release and attachment slice locally verified; release max 25 assets x 256 KiB, discussion max 100 files x 256 KiB; no attachment replacement/deletion.



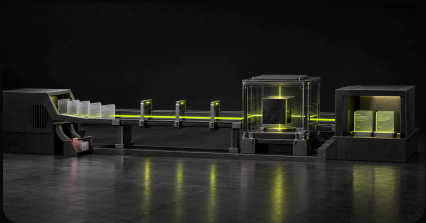
Queues

Make admission durable

ROLE IN GOLF

Purpose in Golf

Buffers evidence IDs into Workflows with durable D1 outbox, bounded retries and reauthorization.

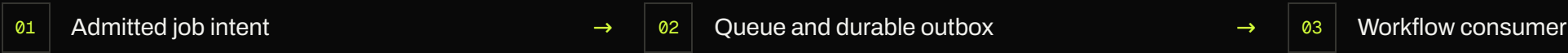


How the workflow uses it

The evidence queue buffers source-bound work before the Workflow consumer starts it. Stable identity and bounded handling preserve the original request across delivery retries.

Current operating boundary

Email/webhook transport currently uses D1 outboxes and maintenance, not Queues.



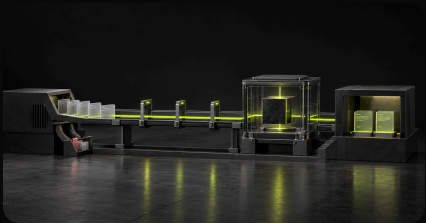
Queues dead-letter queue

Retain exhausted evidence delivery

ROLE IN GOLF

Purpose in Golf

Optional separate queue retains failed evidence deliveries and exposes failure retention.

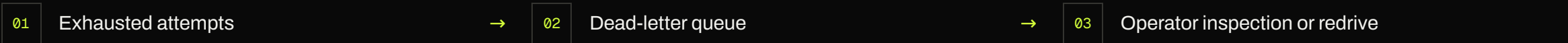


How the workflow uses it

An optional separate queue/consumer records delivery that exceeded its normal attempts. Redrive is an operator decision with fresh authority checks; it cannot fabricate passing evidence.

Current operating boundary

Provisioning implemented on Alchemy; real dead-lettered delivery not exercised on retained installation.



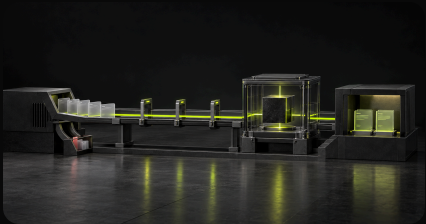
Workflows

Keep stages and outcomes together

ROLE IN GOLF

Purpose in Golf

Coordinates authorization, exact-source tests, agent proposals, report publication, previews and cleanup through durable steps.

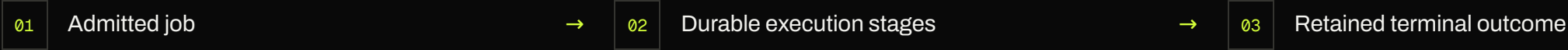


How the workflow uses it

Durable stages reserve authority, start approved compute, retain reports and manage bounded delivery. A provider timeout remains an observed failure/uncertainty, never an assumed success.

Current operating boundary

Bounded concurrency/retention/steps; Workflows coordinate effects but do not grant authority or approve merges.



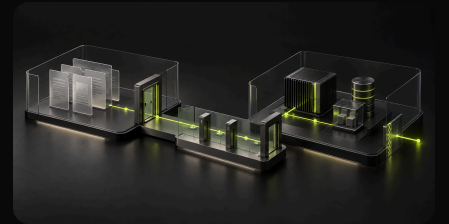
Workers for Platforms

An app preview with its own resources

ROLE IN GOLF

Purpose in Golf

Dispatches isolated PR Worker applications behind the preview gateway, with separate private D1/R2, child hostnames and an outbound-denial Worker.



How the workflow uses it

Dispatch an approved prebundled Worker module with per-preview D1, R2 and signing material. A dedicated Outbound Worker enforces the configured application egress policy.

Current operating boundary

Only approved prebundled module/schema; arbitrary builds/bindings, app cookies/WebSockets, production promotion and multi-tenant scale remain open.

01

Approved Worker bundle



02

Dispatch namespace



03

Isolated preview resources

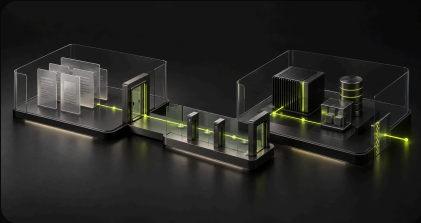
Access / Zero Trust

Identity plus a Golf grant

ROLE IN GOLF

Purpose in Golf

OTP login and approved-email policies gate control/preview domains; service tokens protect machine access; Golf rechecks D1 repository grants and short-lived single-use preview grants.

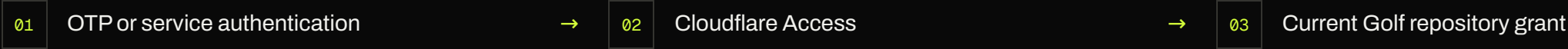


How the workflow uses it

Separate human OTP and machine Service Auth policies protect the control/preview entrypoints. Golf maps verified identity to an already enrolled active account, then checks repository permission.

Current operating boundary

Access admission does not itself grant repository permission; native account lifecycle and broader identity onboarding remain open.



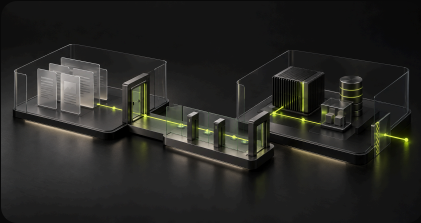
DNS, custom domains and TLS

Protect the actual hostnames

ROLE IN GOLF

Purpose in Golf

Provides branded control/preview URLs and per-application child hostnames; Email onboarding provisions DKIM/SPF/return-path DNS.

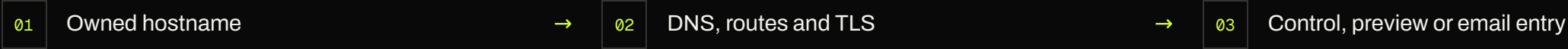


How the workflow uses it

Own-zone control and preview domains receive TLS and approved routing. Email sender onboarding adds DNS records. Alternate endpoints must not bypass the Access and Golf reader boundaries.

Current operating boundary

Selected approved zone/hostnames only; customer vanity-domain lifecycle is separate planned Cloudflare for SaaS work.



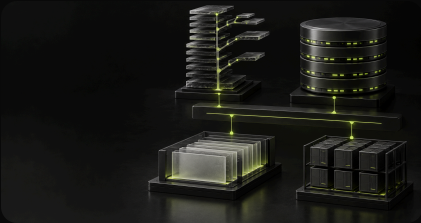
Secrets Store

Trusted authority, scoped value release

ROLE IN GOLF

Purpose in Golf

Keeps management/registry/analytics credentials, app signing key, webhook encryption key and execution-value AES-GCM key in trusted bindings.

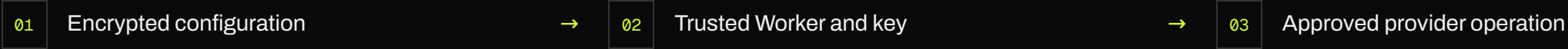


How the workflow uses it

Separate secrets hold provisioner/registry/analytics authority, signing and encryption keys. Repository values are ciphertext in D1 and reach only an exact-approved native PR workflow.

Current operating boundary

Secret rotation procedure and approved external-egress broker remain open; job log masking only detects exact secret text.



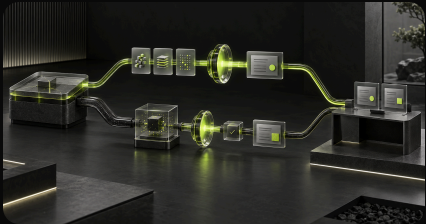
Workers AI

Two inference jobs

ROLE IN GOLF

Purpose in Golf

Runs optional metadata review advice on @cf/cloudflare/clef and coding proposals on @cf/zai-org/glm-5.3-flash through trusted brokers.

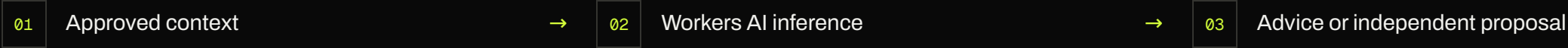


How the workflow uses it

Clef supplies metadata-only advisory PR evidence. GLM 5.3 Flash powers the maintained proposal harness on an independent fork; approved tests and human review remain separate from inference.

Current operating boundary

Advice is metadata-only; proposals change one approved file and are tested in an independent Artifacts fork; per-use-case model selection remains planned.



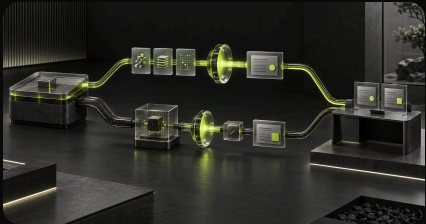
AI Gateway

A policy on inference

ROLE IN GOLF

Purpose in Golf

Private authenticated inference gateway disables prompt/response logs and cache, caps 60 requests/minute and configures 500 cents/day.

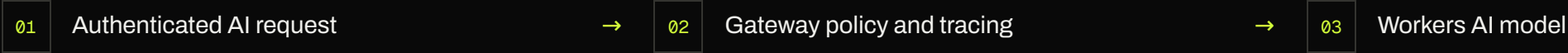


How the workflow uses it

Route authenticated Workers AI calls through a private gateway, with prompt/response logging and cache disabled. The retained configuration sets 60 requests/minute and a \$5/day limit.

Current operating boundary

Rate/spend-limit enforcement not exercised; admin gateway usage UI remains planned; AI remains opt-in.



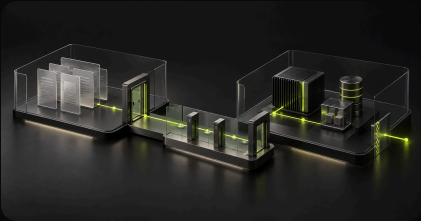
Browser Run

Optional static preview snapshots

ROLE IN GOLF

Purpose in Golf

Optional one-dispatch static-preview PNG capture retained privately with digest checks and current-reader authorization.

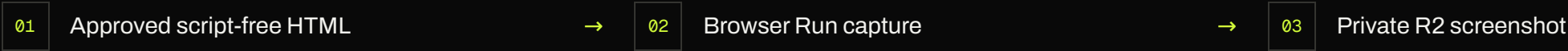


How the workflow uses it

An explicitly authorized snapshot can capture script-free static HTML with external requests denied. A historical hosted proof produced a real PNG; retained captures were not completed at this review.

Current operating boundary

Enabled in the reviewed engineering deployment, with no completed retained captures at this review. Historical hosted proof covers script-free static HTML only; full interactive QA remains open.



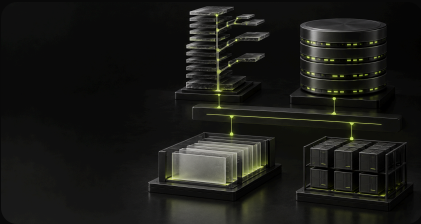
Analytics Engine

Optional evidence metrics

ROLE IN GOLF

Purpose in Golf

Optional sampled evidence-completion counts, report bytes, duration and observed tokens with hashed workspace index and no source/prompts.

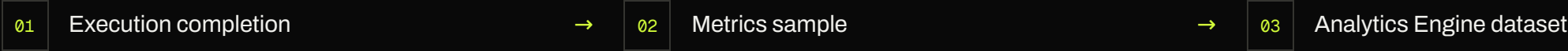


How the workflow uses it

The deployed dataset binding accepts the implemented source path for bounded evidence metrics. Hosted ingestion/SQL readback still needs acceptance; metrics are not quota or billing authority.

Current operating boundary

Source, build and binding checks passed. Hosted ingestion and SQL readback are unverified. Metrics do not govern billing or quotas.



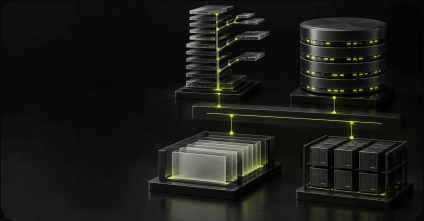
Workers Analytics API

A separate operational read path

ROLE IN GOLF

Purpose in Golf

Operations collector reads requests/errors/subrequests from GraphQL with a separate Account Analytics Read credential.

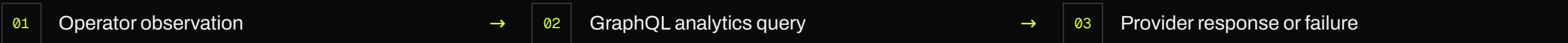


How the workflow uses it

Operations requests installed-Worker traffic through a dedicated account Analytics Read token in Secrets Store. The retained feed has failed collection; configured is distinct from collected.

Current operating boundary

Collection currently fails inside the Worker. The equivalent token/query succeeds externally.



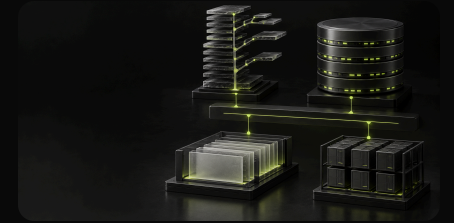
Workers Logs / managed observability

Provider observations with explicit policy

ROLE IN GOLF

Purpose in Golf

Optional sampled logs help diagnose the native deployment alongside local D1 journals.



How the workflow uses it

The retained Worker reports observability enabled and logpush disabled. Invocation/log/query-string/privacy and retention settings remain separately scoped; no complete trace/export consumer is claimed.

Current operating boundary

Provider observability is enabled on the reviewed engineering deployment; logpush is disabled. Wider tracing/export and retention remain separate acceptance.

01 Worker invocation



02 Managed provider logs



03 Operator inspection

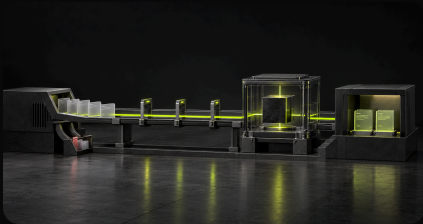
Cron Triggers

Maintenance with a fallback

ROLE IN GOLF

Purpose in Golf

Configured five-minute maintenance for CI intake retry, preview purge, evidence/index reconciliation, webhook/email retries and probes.

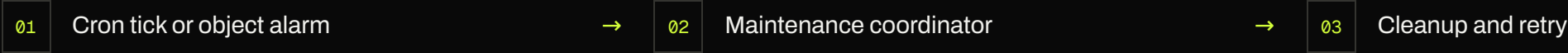


How the workflow uses it

The declared schedule has delivered no events on the retained account. Workspace keeps a five-minute alarm and runs maintenance after ten minutes without a scheduled report; it stands down when cron resumes.

Current operating boundary

Retained account receives no scheduled events; workspace DO alarm supplies maintenance fallback and cause is unresolved.



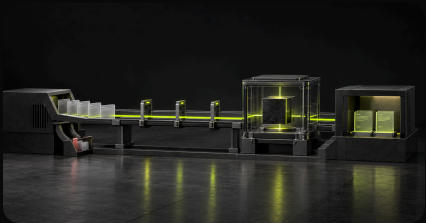
Workers rate limiting

Bound anonymous reads approximately

ROLE IN GOLF

Purpose in Golf

Optional per-network/location approximate throttling protects credential-less public source and clone reads.

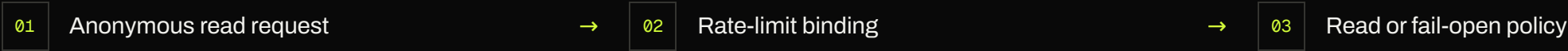


How the workflow uses it

Credential-less public source/clone requests use per-network/location rate counts. Signed-in, credentialed and runner calls are excluded. A limiter error allows the request; this is not a global execution quota.

Current operating boundary

Signed-in, credentialed and runner requests are excluded. Limiter errors allow the request. This is not a security quota.



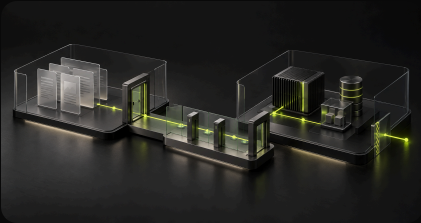
Email Service sending

Notify the enrolled address

ROLE IN GOLF

Purpose in Golf

Consent-based own-Access-address repository subscriptions receive category-and-link notifications from D1 outbox with rechecks, bounded retries and daily attempt budget.

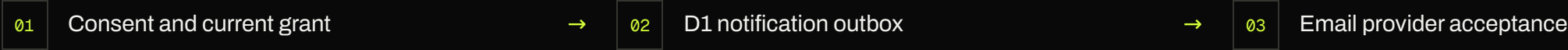


How the workflow uses it

Consent and repository subscriptions fill a D1 outbox. Send from the onboarded subdomain after current account/address/grant checks; record provider acceptance and bounded retry observations.

Current operating boundary

Retained installation provider acceptance verified; inbox receipt unobserved; bounces/complaints/replies/unsubscribe links remain open.



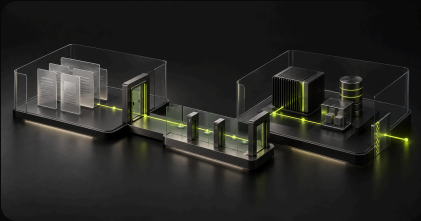
Signed webhooks

Deliver a committed event observation

ROLE IN GOLF

Purpose in Golf

Encrypted repository subscriptions and stable signed deliveries to approved HTTPS receivers; retained Slack test accepted.

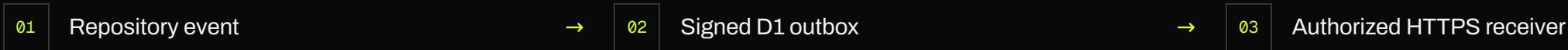


How the workflow uses it

Encrypted subscriptions choose approved HTTPS origins. Sign a stable event document and retain receipt/attempt status. Native Slack delivery uses the accepted text shape; receivers should deduplicate.

Current operating boundary

D1 outbox/maintenance provides bounded retries, not queue-based email/webhook transport. Receiver/event/retry matrix remains bounded.



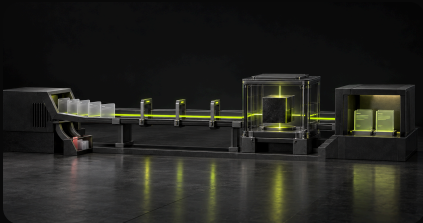
Cloudflare CLI

Provision and verify owned resources

ROLE IN GOLF

Purpose in Golf

cf supplies scoped provider discovery, setup/deploy and readback qualification; Alchemy optionally provisions equivalent reviewed native resources.

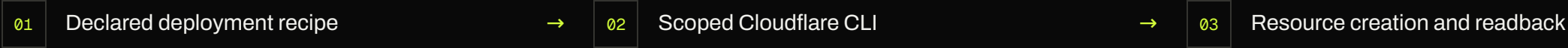


How the workflow uses it

Alchemy defines the stack; native cf supplies supported operations and deployment. Additive migration, token renewal, binding/domain readback and ownership-aware teardown keep the installation concrete.

Current operating boundary

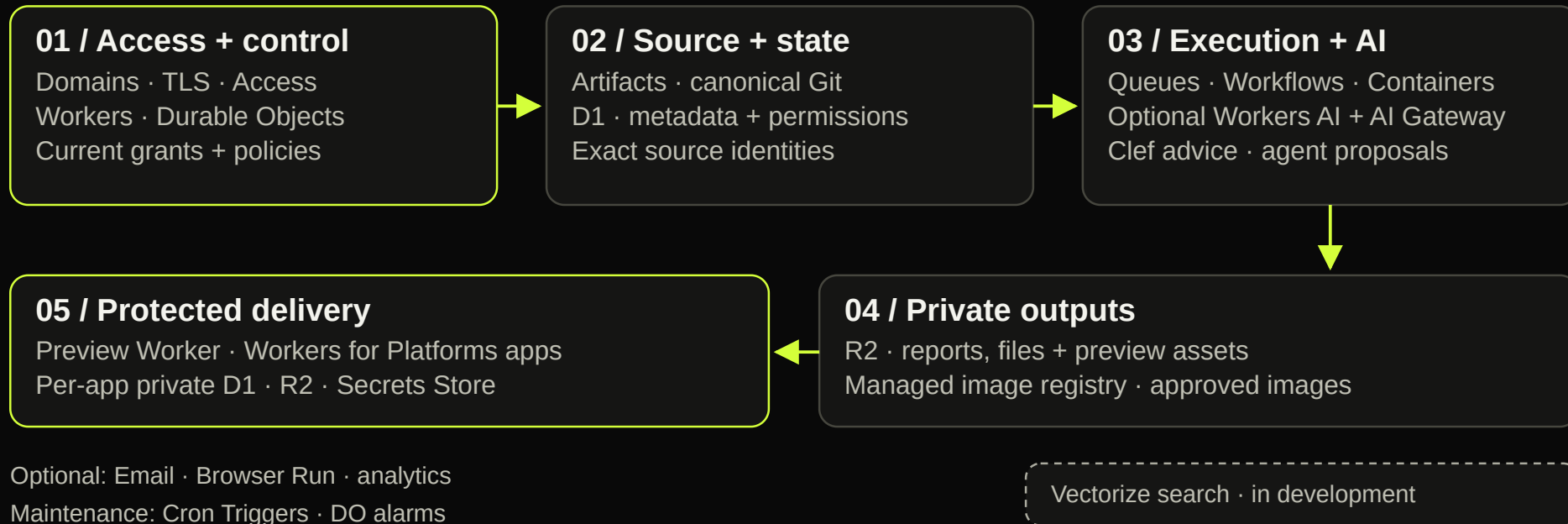
Alchemy beta and cf beta are deployment dependencies only; private state/journals require careful ownership and teardown inspection.



A platform built from managed primitives.

Each service has a specific role. Golf retains current authorization.

golf. CLOUDFLARE / NATIVE PLATFORM



[Editable architecture diagram](#) · [Open full size](#)

Code. Check. Review. Preview.

Follow one exact change through the workspace.

01

01 / Source

Select the repository, branch and exact commit.

02

02 / Change

Open an issue or same-repository PR and request review.

03

03 / Check

Run an authorized profile and inspect the terminal report.

04

04 / Preview

Publish an allowed protected preview and inspect the result.

Search beyond exact matches.

Semantic code and issue search is being added.

01

Workers AI embeddings

Create semantic representations from approved source content.

02

Vectorize

Index and query those representations to find related code and issues.

03

Current reader access

Filter results by live repository authority and propagate deletion/revocation.

A developer preview with real evidence.

Dated engineering proofs cover selected Git, test, proposal and protected-preview paths. Production readiness still needs testing.

01 Demonstrated Hosted Git, collaboration, approved tests, Clef advice, scoped proposals, protected previews, email acceptance and secret-to-step delivery.	02 Incomplete or degraded Cron delivery and analytics collection; Analytics Engine ingest; retained screenshots; broader role/load/cleanup matrices.	03 Next acceptance Full parity, protected merge, production CD, native/Forgejo recovery, tenant onboarding and scale. Vectorize search is in development.
---	--	---

YOUR NEXT MOVE

Try Golf for yourself.

Start with a browser simulation, then install Golf to evaluate real workflows.

01

Browser simulations

gitgolf.app/demo: explore local and Cloudflare interfaces with sample data.
No backend or live execution.

02

Choose your deployment

Docker Compose or Golf's Helm chart for portable hosting. Use the native Alchemy recipe in your own Cloudflare account.

03

Evaluate real work

Enroll a user and grant repository access on your installation. Check an exact commit and inspect its report.
docs.gitgolf.app

[gitgolf.app/try ↗](https://gitgolf.app/try)