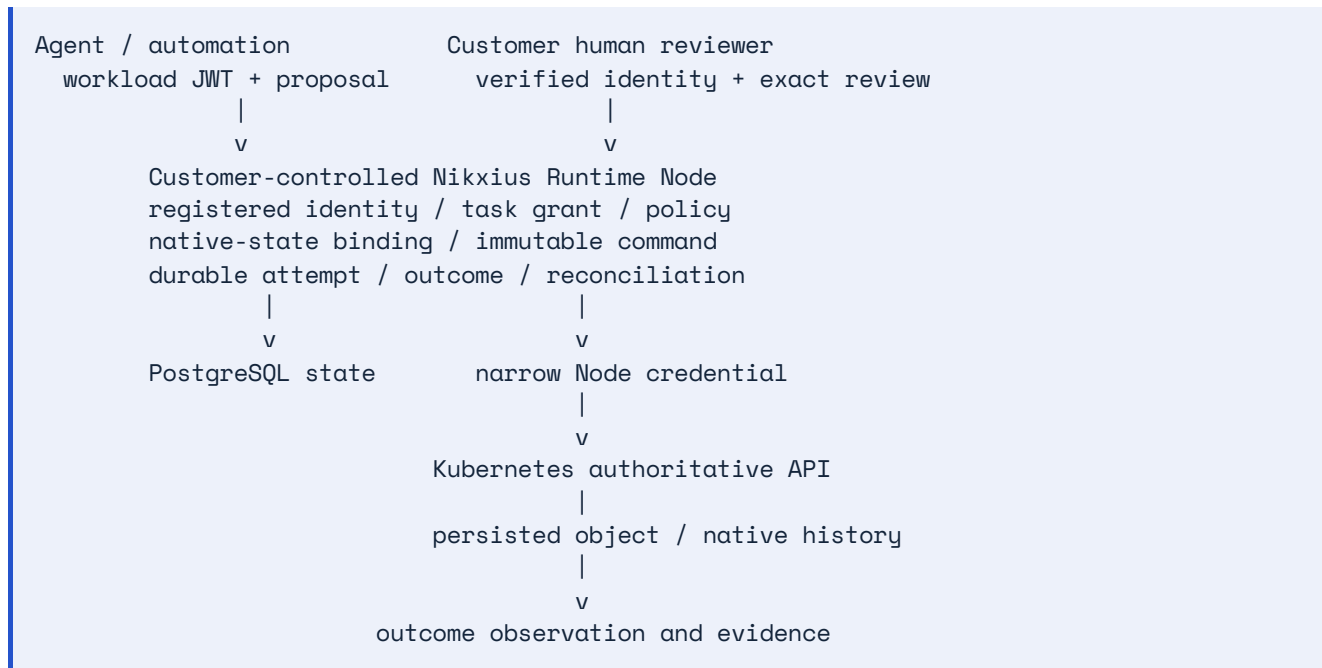


Nikxius

DESIGN-PARTNER EVALUATION · PROPOSED

One operation, one durable record

Technical architecture · Customer-controlled Runtime



Customer IdP supplies verified identities. Customer secret management supplies protected credentials. Native RBAC/admission and existing writer ownership remain authoritative. Monitoring, SIEM and GRC can consume exported records through customer integration; no turnkey SIEM/GRC connector is claimed by this diagram.

Control flow

The workload submits a typed request, grant reference and stable idempotency key. The server derives tenant and principal from registered issuer/subject mappings. It independently reads Kubernetes, checks enrollment and authority, and freezes the target, effect, policy and native UID/resourceVersion. Required human review binds exact command/dispatch hashes and the current operation version.

Before sending a protected mutation, PostgreSQL records admission, reservation and dispatch identity. The Node constructs a conditional native patch. It accepts no arbitrary URL, YAML, shell command or caller-supplied patch. A lost response does not authorize another mutation.

The Node records the persisted native response or retained causal history. Read-only reconciliation can resolve an unknown commitment only with sufficient evidence. A current GET showing the expected image is insufficient on its own.

Read each state dimension

Dimension	Meaning
Lifecycle	PROPOSED, AWAITING_APPROVAL, REVALIDATING, ADMITTED, DISPATCH_RECORDED, PENDING, UNKNOWN, RESOLVED, DENIED.
Commit	not_dispatched, committed, rejected, unknown.
Observation	not_applicable, pending, converged, degraded, superseded, unobserved.
Reservation / integrity	Task/resource capacity and separately recorded unchecked, matched OR mismatch invariants.

RESOLVED does not mean success. committed does not mean healthy. A committed invariant mismatch remains an incident with consumed authority.

Integration boundary

The first deployment uses one Node plus PostgreSQL. API and worker may run together. Browser sessions are process-local; the initial evaluation is not a claim of multi-replica availability. PostgreSQL and Kubernetes share no transaction. Worker leases protect local ownership, while the native conditional request protects its frozen baseline.

A GitOps controller that owns the field must be part of the design. Do not create a second uncoordinated writer. If the customer's approved GitOps path already meets the contract, that path is the comparator to beat.

Source: docs/runtime/API.md, OPERATIONS.md, DEPLOYMENT.md, RECOVERY.md; docs/security/TRUST_BOUNDARIES.md in the evaluation checkout. No hosted Nikxius control plane is required for this Runtime path.