

Nikxius

DESIGN-PARTNER EVALUATION · PROPOSED

Rollback is a new operation

Kubernetes workflow · One Deployment, one permitted prior image

An AI/SRE agent proposes restoring a Deployment container to a prior permitted image. The agent does not receive broad cluster write credentials. Nikxius checks an exact rollback contract; Kubernetes remains authoritative for the conditional mutation and native state.

Bind the relationship

`kubernetes.deployment.rollback_image.v1` requires an explicitly authorized immutable image and `compensatesOperationId`. The earlier operation must be committed in the same tenant, for the same native target/UID, with the appropriate reversed before/after images. An arbitrary old registry digest is not sufficient.

The contract binds the registered cluster, namespace, Deployment, container, native UID/version, image, earlier operation, grant, review policy and stable idempotency key. Customer enrollment must permit the relationship. Use actual observed values; the following is a shape, not an executable grant:

```
{
  "operation": "kubernetes.deployment.rollback_image.v1",
  "target": {
    "cluster": "evaluation",
    "namespace": "evaluation",
    "deployment": "sample-api",
    "container": "api"
  },
  "input": {
    "image": "registry.example.com/sample@sha256:<prior-digest>",
    "compensatesOperationId": "<earlier-committed-operation>"
  },
  "grantRef": "<sponsor-issued-grant>",
  "idempotencyKey": "<stable-task-specific-key>"
}
```

Illustrative tokens above must be replaced from the local runner's actual record. The customer receives a runnable generated example, not these placeholders as an install step.

Review, execute, recover

The Runtime independently reads current state and freezes the exact command. Required approval binds current hashes/version, not “allow a rollback sometime.” Before dispatch it revalidates authority and state, persists attempt identity and constructs a conditional patch.

If the native response establishes the intended mutation, record `committed`. Observe rollout separately. If the response is lost, retain `UNKNOWN` and the reservation; read-only reconciliation must establish the original causal transition. A current matching image or inherited annotation alone cannot establish attribution.

Failure cases to see in the evaluation

Case	Expected boundary
Different target/image/earlier operation	Old grant cannot authorize it.
Resource recreated or concurrently edited	Frozen UID/version cannot silently rebase.
Permission expired/revoked before dispatch claim	New dispatch refused; already accepted writes are not recalled.
Same key, same immutable request	Same operation identity; changed payload conflicts.
Lost response or interrupted worker	Preserve attempt and uncertainty; do not blindly patch again.
Accepted mutation, unhealthy application	Commit remains committed; health and further corrective action require separate assessment.

A rollback may itself fail or remain `UNKNOWN`. If GitOps owns the image field, use its approved write path or select another valid evaluation target. Source: `docs/runtime/OPERATIONS.md`, `API.md`, `RECOVERY.md` and the acceptance runner supplied with the source checkout.