



Uncertain-write test session

Test uncertain exception writes, duplicate requests and recovery using a completed holdings-reconciliation example.

Purpose

Test uncertain exception writes, duplicate requests and recovery using a completed holdings-reconciliation example.

For Investment-operations and engineering leads granting an agent limited write access.

How to use

Read the completed hypothetical example, replace all teaching values with approved test inputs, agree expected results before running, then retain observed evidence and the authorised decision. Work in a non-production environment.

Session setup

Use a non-production environment and an approved synthetic holdings pair. Operations defines the business operation and permitted action. Engineering identifies the actual commit boundary, authoritative result source and duplicate constraint. Record the API, rule, role and environment versions before running.

Completed hypothetical example

R-207 compares 1,000 internal units with 990 broker units at the same close under rule 1.3. Difference: 10 units. The agent may create a pending exception but cannot approve it or alter holdings. Persist key R-207-EX-01 and the exact payload before sending. The example retains its binding for 90 days, limits automatic retries to 24 hours and keeps a durable business uniqueness check. These invented intervals need replacement with the actual service contract.

Run and inspect

- Stale broker date: Reject comparison; no exception
- Lose reply after commit: Authoritative result resolves to EX-184; one pending exception
- Same key and same payload: Return EX-184 without a second record
- Same key, difference changed to 12: Reject mismatch; EX-184 still records 10
- Two concurrent identical calls: One creator; both callers resolve to the same result
- Crash before commit: Neither exception nor operation result exists
- Reply lost after commit: Exception and operation result both exist
- Agent attempts approval: Denied; pending status and holdings unchanged
- Result service unavailable: UNKNOWN; stop dependent writes and assign recovery
- Retry after allowed window: No automatic new creation; owned recovery

Completed failure and repair

The initial candidate performs an unprotected lookup then insert. Two simultaneous requests create two records. The corrected design uses a unique business-operation constraint and transactional creation with its result. The hypothetical retest leaves one EX-184 and returns it to both callers. Actual

engineering must reproduce the test at the real storage boundary. For an external side effect, also test the destination's deduplication and durable outcome tracking.

Recovery record

At 09:03 the reply is lost; at 09:04 the result service is unavailable. Mark UNKNOWN and assign the investment-operations owner. At 10:20 service returns: authoritative lookup finds EX-184, matching payload digest and one 10-unit pending exception. The owner records reconciliation and permits resumption. A conflicting or absent result needs the documented recovery decision; never invent a new key merely to escape uncertainty.

Record your result

For each test, capture operation identity, payload, snapshots, role, tool version, injected fault, expected state, observed state, result reference and decision owner. Preserve failed tests and the repair/retest history. Decide whether only pending-exception preparation may be enabled; approval, holdings and valuation changes remain outside this example. Measure preparation, review, exceptions and recovery together.

Sources

- AWS Builders Library: Making retries safe with idempotent APIs (<https://aws.amazon.com/builders-library/making-retries-safe-with-idempotent-APIs/>)
- AWS EC2 idempotency documentation (<https://docs.aws.amazon.com/ec2/latest/devguide/ec2-api-idempotency.html>)
- FINBOURNE OMBA announcement (<https://www.finbourne.com/omba-runs-finbourne-agentic-ai-in-production-across-daily-investment-operations/>)
- ESMA AI investment-services guidance announcement (<https://www.esma.europa.eu/press-news/esma-news/esma-provides-guidance-firms-using-artificial-intelligence-investment-services>)

Limits

Proposed operating design with invented cases and outcomes. No observed client results or compliance determination. Substitute actual policy, permissions, source versions and API behaviour. Human implementation and publication approval remain required.