

Certified image retirement

Vikrant Rathore, with assistance from Ronak Rathore.

This argument covers R3.4 image retention; it is not the complete R2 consensus refinement or a production qualification decision. `ImageRetirement.tla` checks three voters and two image prefixes, including reordered receipt delivery and learning a chosen seal. Its negative controls remove each of the successor, active-image and predecessor-image protections.

Assumptions and composition

`SnapshotIdentity` establishes that a certificate contains a matching quorum of authenticated voter receipts. `ManifestDurability` establishes that a receipt follows durable image and manifest publication. Those receipts can remain in messages after a newer seal permits deleting their old images. Consequently the retention claim applies to the latest chosen certificate, not every historical certificate. Durable storage survives process failure; permanent disk loss and loss of a majority require the fenced recovery procedures in R4.

A chosen seal changes the retained maximum only monotonically. A voter may delete an advertised image at prefix p only after observing a chosen seal at $q > p$. Thus, if C is the largest chosen prefix, no image counted in C 's receipt quorum can have been deleted: deleting one would require an already chosen prefix larger than C , a contradiction. This argument does not depend on a bounded log length. Delayed older receipts cannot reduce the chosen maximum. In the model, `Capture` abstracts successful durable publication before a receipt; `Seal` abstracts choosing a valid certificate, and `Learn` represents local observation.

`retire_snapshot_image` in `src/durable/image_retire.odin` checks the authoritative root catalog and protects both `generation_image_name` and the image referenced by the exact predecessor's verified descriptor. `image_retirement_candidate` requires a strict successor for locally captured images. Neither sorting file names nor listing directories establishes ownership. Incoming copies are a separate class: the receiver does not advertise a receipt for that copy, and may delete it if no active transfer, current generation or predecessor uses it. The bounded model covers advertised images; focused implementation tests cover this incoming-copy distinction.

Ownership is committed with FULL durability before creating a managed image. File deletion and directory synchronization precede removal of its inventory entry. Crashes before completion therefore retain an idempotent cleanup task. This uses the same deletion/sync/forget ordering checked by `GenerationRetirement`, with native SIGKILL checks at all three image boundaries. A failed or ambiguous inventory commit stops service rather than losing a required persistence obligation. File-system owners who replace managed paths concurrently are outside the supported writer model; the stable store guard serializes supported writers.

Evidence and limits

`formal-image-retirement-local.json` records the pinned checker, exact model hashes, exhaustive bounded result and required counterexamples. `image-retirement-local.json` covers active/predecessor/unsealed receipt retention, abandoned incoming copies, transfer exclusion and refusal to adopt foreign files. `image-retirement-crashes-linux.json` covers deletion, directory sync and inventory commit interruption, preserving acknowledged rows, promises, accepted votes and IDs. `live-image-retirement-linux.json` checks three live compaction cycles with two healthy voters, exact protected paths, returning offline voter and full restart. These results belong to the identified source increments, not a future final release candidate. The aggregate history quota remains a separate part of R3.4.