ARF Authority Witness

Restoring authority without spending twice

An old backup can recover a document exactly as it was. A grant has a harder problem. Between backup and failure, a worker may have spent its allowance, lost access or handed a job to a successor. Restoration has to account for that intervening history.

Give the witness an independent copy

The authority-witness design uses an independently administered store with authenticated append and retrieval. Each accepted record advances a sequence and digest. A durable receipt gives the authority writer a specific commitment to retain. A verifier can compare its local history with a commitment held outside the system it is inspecting.

Keep the capture signer, the holder of a checkpoint and the restorer distinct in the evidence. A signature over a local export identifies its signer. A prior independent commitment adds a comparison point that survives loss or alteration of the writer's own store.

Interrupt the restoration in two places

The attended authority recovery exercise stopped the process during a database write. It also tested a committed reconstruction whose reply never reached the caller. In both cases the gate on ordinary runtime remained in force. The recovery command supported exact retry and carried the already-spent allowance forward.

Independent verification checked 94 signatures, 45 canonical records and 323,783 exact bytes. It rejected 26 altered cases. Wrong expected history, domain, trust and maintenance identity were among the refused inputs. A stopped witness was bounded by the original command deadline.

Decide when work may resume

Recovering the authority database settles what it says about past grants and spend. Releasing the runtime also depends on current witness continuity, reconciliation with the target and exclusion of obsolete writers. The SDD assigns that release a separate decision.

For a customer exercise, have one operator restore and another decide whether to reopen the work. Give the second operator the expected history and the target observation. Ask them to point to the last accepted spend and the evidence that the former owner can no longer act.

Recovery evidence to place side by side

Question	Evidence	Why it matters
Which history did we expect?	Witness identity, expected domain and prior commitment.	Selects the authority history being restored.
Which bytes came back?	The verified canonical record sequence.	Accounts for the state rebuilt by the command.
What happened to spent allowance?	The recovered state and the prior spend.	Lets the operator check that the budget did not reset.
Can the job reopen?	Current continuity, target reconciliation and writer exclusion.	Informs the separate decision to release the recovery gate.

Sources and evidence

Reconstructing authority from witnessed history · Implementation record · Offline verification of a checkpoint