7.2 Standby

Intent

Structure a system so that the service provided by one component can be resumed from a different component.

Also Known As

Disaster Recovery, Backup Site

Motivation

In many system implementations it is only cost-effective to implement a single, coarse recovery mechanism that will suffice for all forms of fault or failure, up to and including the complete destruction of a component (as by fire or other environmental failure).

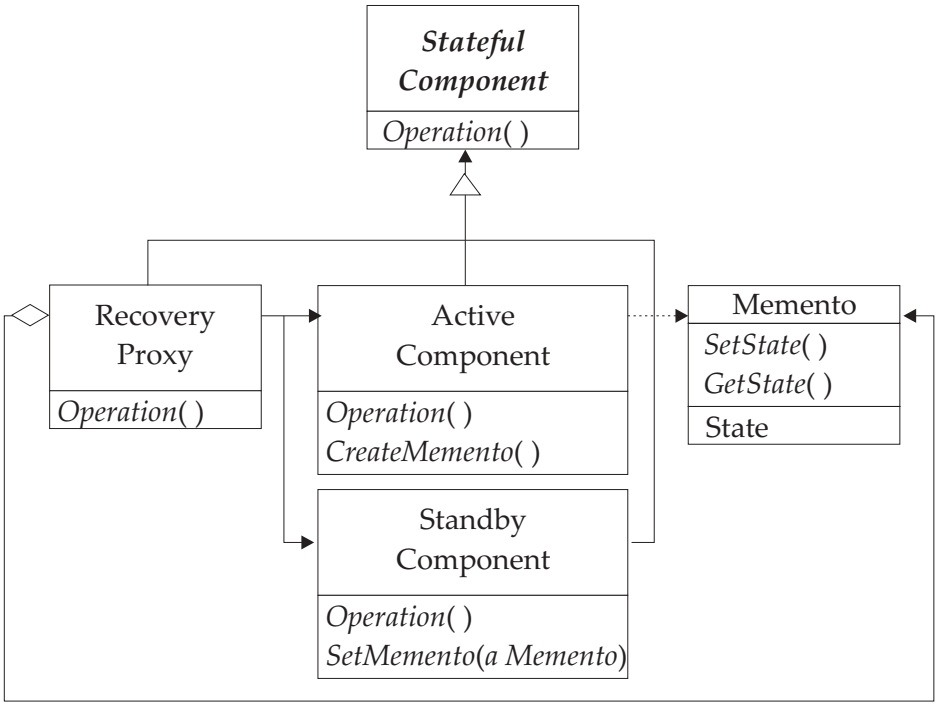
Applicability

Use Standby when:

- It is not acceptable for a single component failure to cause a system service outage.
- It is anticipated that a failed component may not be recoverable, but a similar or identical backup component is available.
- A small number of transactions occurring between the time a component fails and the time service is restored using a backup component are irrelevant or inconsequential, or can be recovered and reapplied.
- Employing a duplicate component is economical.
- Externalizing component state is feasible.

Structure

The Standby pattern consists of one active Recoverable Component and at least one Standby Recoverable Component. When the Standby is activated, the Memento (or Mementos) of the active component are consumed by the State Recovery facility of the Standby component, which ‘‘restores’’ the state to the Standby component and activates it.



Participants

- Active Component

  A Stateful Component. Performs operations on behalf of clients. Periodically saves state to Memento.

- Recovery Proxy

  Proxy [GoF] for Active and Standby Components. A Stateful Component. Caretaker for Active Component's Mementos. Initiates creation of Mementos when Active Component state changes. Detects failures and initiates recovery by instructing Standby Component to restore state from Memento and routing operations to Standby Component.

- Standby Component

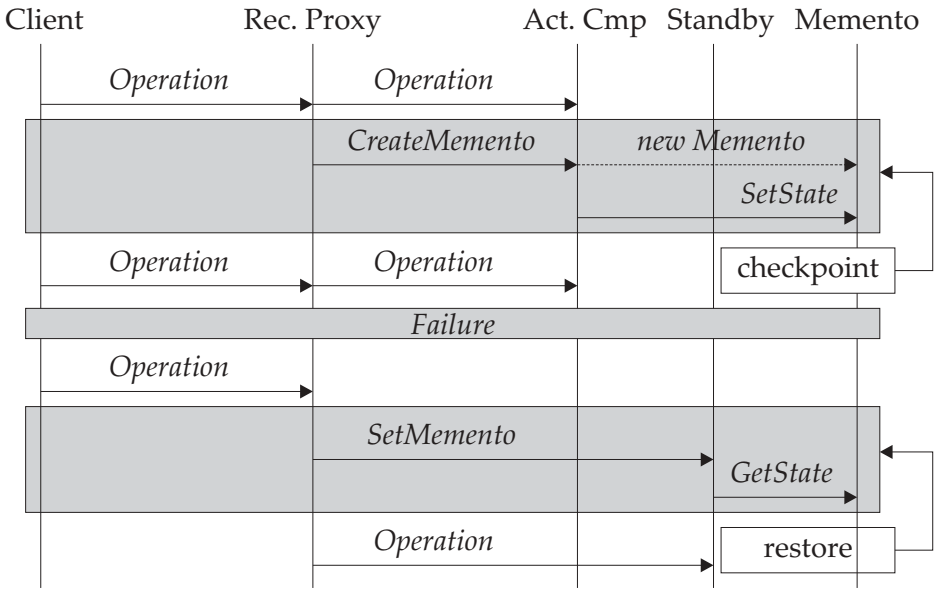
  Waits for failure of Active Component. Upon failure, restores state from Memento and activates.

- Memento

  A Memento [GoF]. Encapsulates the state of the Active Component. Used by the Standby Component to restore the system's state and resume operations.

Collaborations

- Recovery Proxy responds to client requests for operations and dispatches them to the Active Component.
- From time to time, Recovery Proxy instructs Active Component to checkpoint its state by creating a Memento.
- In case of a failure of the Active Component, Recovery Proxy activates the Standby Component by restoring the Memento's state to it and routing requests to it instead of the failed Active Component. Note that any transactions which the failed Active Component executed after its last checkpoint will be lost.



Consequences

Use of Standby:

- Improves system resistance to component failures.
- May introduce a substantial delay between component failure and standby activation.
- Increases system complexity. Creating the Memento may require the creation of work queues or other transaction management constructs to ensure consistency of the state data stored in the Memento.
- May impair system latency or throughput if creation of a checkpoint requires processing to pause or stop.
- Allows loss of a small number of transactions.
- May require substantial resources for storage of Memento information.
- Increases system cost by requiring at least one non-operational component.

Implementation

A wide variety of implementation approaches are possible. Examples include:

- Offsite backup

Known Uses

Offsite disaster recovery services often implement instances of the Standby pattern.

Related Patterns

Standby is a Checkpointed System [TG_SDP] with an identical spare Recoverable Component.

Standby uses a Memento [GoF] to communicate state information from the active component to the Standby Component when recovery is required.