Clove: Failure-Aware ML Research Pipeline Demo

This document describes a real-world, working demonstration built using Clove. The goal of the demo is to showcase Clove as a research-grade infrastructure runtime for executing machine learning pipelines with strong guarantees around isolation, failure handling, and reproducibility.

Problem Statement

Machine learning research pipelines are inherently fragile. Training jobs crash due to out-of-memory errors, misconfigurations, or unstable code. Partial results are often lost, reruns are non-deterministic, and failures require manual intervention. This demo addresses these issues by treating ML experiments as supervised OS-level workflows.

Demo Objective

Build a reproducible, isolated, and failure-aware ML research pipeline where each stage is executed as a supervised process with explicit dependencies and observable state.

Pipeline Workflow

- Load Dataset
- Preprocess Data
- Train Model (long-running, failure-prone)
- Evaluate Model
- Generate Report
- Archive Artifacts

Execution Model

Each pipeline stage runs as an isolated OS process managed by the Clove runtime. Processes are subject to resource limits, timeouts, and supervision. Failures are detected via exit codes and signals, triggering retries or fallback strategies.

Failure Handling

The training stage intentionally triggers a realistic failure (e.g., out-of-memory). Clove detects the failure, terminates the process, logs the event, and retries training with a modified configuration such as a smaller batch size. The pipeline continues without manual intervention.

Reproducibility and Auditability

Every run produces a complete set of artifacts including configuration files, dataset hashes, model checkpoints, evaluation metrics, and an execution trace. This ensures experiments are fully reproducible and auditable.

Why This Matters

This demo demonstrates how Clove elevates ML experimentation from ad-hoc scripting to a robust research infrastructure system. The same pattern generalizes to safety-critical

domains such as healthcare ML, where correctness, isolation, and traceability are mandatory.