ARF Agent Execution Cells

# A disposable worktree with a durable receipt

A reviewer wants one more failing test before accepting a patch. The worker needs a checkout, a test runner and a way to return the result. Giving it the rest of the release environment would make the most consequential part of the job harder to explain.

## Name the assignment before the machine

The execution-cell design starts from a job, a sponsor and a lease. An image supplies the permitted tools. A controller owns creation, fencing, checkpointing and destruction. The initial managed-worker design selects Linux KVM with Firecracker and its jailer. Image qualification, host limits and controller generation are part of that specification.

Bind a worker identity to the assignment and allow the destinations the test actually uses. Attach paths also need scope. An operator attaching to inspect a failure is performing a different action from an agent asking the command broker to run the test.

## Put the effect outside the worker

The command broker evaluates the tool request at its boundary. The credential broker can supply scoped access to the executor when the operation needs it. The credential value stays out of the worker conversation. A filesystem observer provides a distinct account of the resulting file activity. Together these components let the reviewer follow an effect from request through observation.

For a first exercise, give the agent a private test fixture and permission to return a report. Have it request publication after the report is ready. Inspect the denial and the bounded work the operator still allows, such as recording a handoff.

## Verify the teardown

Close the lease, try an ordinary follow-up through that lease and inspect the controller's decision. Check for any effects already in flight at the boundary. Hand a second reviewer the evidence and ask them to recover the test input after the temporary workspace is gone.

The native code inventory includes a cell gateway, runtime and filesystem observer. The platform design adds qualification of the full guest, host and recovery boundary. The acceptance exercise joins those responsibilities at the point where the team will actually run its workers.

## A cell's working life

| Stage | Owner in the design | Acceptance question |
| --- | --- | --- |
| Admit a worker | Cell controller and image profile | Which job owns this lease and which tools can it reach? |
| Attempt an effect | Broker and designated executor | Which grant covers this destination? |
| Fence and close | Controller with current generation | Can an old attachment still cause an effect? |
| Read the work later | Reviewer with evidence access | Can the finding be traced to its test input after teardown? |

## Sources and evidence

Execution cells and the guest qualification · Implementation record · From file event to restorable bytes · Implementation record