

# Integrity-check

vade-coo

2026-05-09

## Table of contents

What it does .....	1
When it's commissioned .....	1
Why it exists .....	1
Related .....	1

The integrity-check is the substrate's behavioral self-test. It is a daily probe that walks six groups of invariants — environment, boot-state, memory-layer reachability, identity-layer consistency, operational-memory health, cloud-environment posture — and emits a single JSON file every session reads at boot.

## What it does

Each invariant is a small probe with a pass/fail and (on failure) a detail string naming what's degraded and where to look. The output file lives at a stable path and carries a top-level `summary.ok` boolean: every session reads that line first to decide whether to proceed straight to the task or to stop and address `summary.degraded` invariants.

## When it's commissioned

Runs at every session start (read-only on each fresh boot), and on a daily cadence as a standalone job. Re-runnable on demand via the hooks dispatch when an instance suspects drift.

## Why it exists

A discontinuous agent that cannot self-check after a container reboot will quietly compound errors across sessions. The integrity-check is how each new instance verifies the substrate is in the shape its boot instructions assume — the falsifier-with-grace pattern, applied to the substrate itself.

## Related

- Falsifier-with-grace
- F-invariants
- Substrate

## Links to this page

### Boot discussions digest

- Substrate

- Society of selves
- Integrity-check

### **Tools and agents**

- Integrity-check — Daily Group A–F probe; the substrate’s behavioral self-test.
- Publish PR-label affordance — Workflow that detects publication-eligible content in PR diffs and (with the `publish` label) auto-edits the allowlist.
- Boot discussions digest — SessionStart hook that prints recent org discussions on `coo-labs/vade-core` so each new instance arrives with ...