

Hallucination gate URL host-scope — MC #107370

MC #107370 — live JAR/runtime verification

Verified: 2026-08-21 13:03-13:10 CEST

Canonical repo: `/Users/makinja/system`

Active launcher: `/Users/makinja/.claude/hooks/alai-hooks`

Status at preflight: paused, unassigned; recorded #107370 PID markers were dead.

What was uncertain

The source fix in `HallucinationDetector.kt` had been committed, but an earlier review found that the auto-validate worktree tested a rebuilt native binary while the active launcher actually executes:

```
java -Xss128m -jar $HOME/system/tools/alai-hooks/build/libs/alai-hooks-1.0.0.jar
```

Therefore source/native PASS was not enough; the canonical JAR and live launcher needed direct proof.

GPT-5.6 high isolated JAR rebuild

Builder worktree:

```
/Users/makinja/system/.claude/worktrees/codecraft-105500
```

Builder evidence:

```
/Users/makinja/system/.claude/worktrees/codecraft-105500/evidence/107370/gpt56-high-jar-build-2026-08-21.md
```

The wrapper remains broken because empty quoted JVM option variables are passed as an empty main-class argument. The builder used installed Gradle 9.3.1, matching `gradle-wrapper.properties`, without editing or weakening the wrapper/gates:

```
gradle --no-daemon --no-build-cache --rerun-tasks jar
BUILD SUCCESSFUL
```

Forced recompilation and jar tasks both executed. The resulting JAR:

```
path: /Users/makinja/system/.claude/worktrees/codecraft-105500/tools/alai-
hooks/build/libs/alai-hooks-1.0.0.jar
sha256: df0f38d5a86c23b8e5564bd7def2cbaeb280da79ba5fa5b76d87086dfcfa337e
size: 1,930,197 bytes
mtime: 2026-08-21 13:09:07 CEST
```

The pre-build JAR in that worktree already had the same hash. `--rerun-tasks --no-build-cache` proved this was byte identity, not a skipped stale build. `HallucinationDetector.class` is packaged and `javap` shows `java.net.URI.create/getHost/getPort/getPath` bytecode.

Builder JAR tests:

```
#107370 URL scope: 7 passed, 0 failed
existing alai-hooks regression: 29 passed, 0 failed
Gradle compile/check: BUILD SUCCESSFUL
```

Canonical artifact identity

Canonical JAR:

```
path: /Users/makinja/system/tools/alai-hooks/build/libs/alai-hooks-1.0.0.jar
sha256: df0f38d5a86c23b8e5564bd7def2cbaeb280da79ba5fa5b76d87086dfcfa337e
size: 1,930,197 bytes
mtime: 2026-08-21 10:50:13 CEST
```

The canonical JAR is byte-identical to the forced, independently rebuilt worktree JAR. Another session had already rebuilt the correct canonical artifact, so copying/deploying it again would only create duplicate risk. No copy or deployment was performed.

Direct canonical and live tests

Canonical JAR:

```
PASS localhost:9621/uploads/batch.json      -> blocked, exit 2
PASS localhost:9621/upload                  -> blocked, exit 2
PASS localhost:9621/documents/text          -> allowed, exit 0
PASS external host /9621/uploads/...        -> allowed, exit 0
PASS external host /uploads/...             -> allowed, exit 0
PASS second external /uploads/...           -> allowed, exit 0
PASS localhost:11434/uploads/...            -> allowed, exit 0
RESULT: 7 passed, 0 failed
```

Active launcher `/Users/makinja/.claude/hooks/alai-hooks` against the same matrix:

```
RESULT #107370 localhost:9621 URL scope tests: passed=7 failed=0
```

Full existing active-hook regression:

```
Results: 29 passed, 0 failed
```

JAR package/bytecode:

```
com/alai/hooks/HallucinationDetector.class
java/net/URI.create
java/net/URI.getHost
java/net/URI.getPort
java/net/URI.getPath
```

Verdict

PASS for live runtime behavior. The active hook launcher executes the canonical JAR, that JAR is byte-identical to the forced GPT-5.6 rebuild, and both the focused 7/7 matrix and existing 29/29 regression pass through the active launcher.

No code, active launcher, settings, MC marker, credential, cloud resource or deployment target was changed during this verification.

Revision #1

Created 2026-08-21 11:15:40 UTC by John

Updated 2026-08-21 11:15:40 UTC by John