

Buzz-routerproef agentwerelden

Uitkomst

De bestaande private Buzz-omgeving heeft nu een kleine, fail-closed router voor Codex, Claude, Kimi en een geïsoleerde Hermes-route. Buzz is alleen communicatie; code, profielen en werkmappen blijven gescheiden. Voor Antigravity/Gemini is een officiële technische ACP-route gevonden, maar de koppeling is bewust niet uitgevoerd: Googles actuele voorwaarden verbieden Antigravity-login via software van derden.

Daarnaast is een **neutrale statusbrug** end-to-end getest met synthetische data. Antigravity kreeg daarbij geen Buzz-identiteit. De brug gebruikte ook geen ACP, third-party OAuth, nieuwe login of Antigravity-API. De fixture-route is bewezen. Een echte first-party Antigravity-hook is nog niet uitgevoerd.

Bewijs

- Private kanaal: `agent-router-proef-2026-09-28` .
- Kimi: één direct bericht, één juist antwoord, nul onverwachte antwoorden.
- Hermes: één direct bericht, één gesigneerd antwoord, nul onverwachte antwoorden; een herhaalde toolcall werd als `already_published` genegeerd.
- Appel-route: één bericht naar actieve eigenaar Codex, één antwoord `APPEL_EXECUTOR_OK` , nul onverwachte antwoorden.
- Dezelfde `message_id` opnieuw aanbieden gaf nul extra antwoorden.
- Broadcast-ack controleerde vier kanaallidmaatschappen zonder modellen wakker te maken.
- 17 lokale router/radar/replytool-tests zijn groen.
- De aparte statusbrug heeft **30 van 30** unittests doorstaan.
- De volledige Python-suite telt 44 tests: 43 geslaagd en 1 gedocumenteerde skip, zonder fouten.

- De eerdere cockpitmeting na de voorwaardencontrole had nog de ruwe, niet-ontdubbelde teller `15 events · 5 bewezen · 3 gestopt/gefaald` .
 - De actuele Hermes Taakcockpit toont na de v2-statusbrugproef `17 events · 3 bewezen · 3 gestopt/gefaald` .
 - De statusbrugactiviteit staat als `status_verified` . De teller `uniek bewezen` ontdebelt dezelfde combinatie van bericht-id en bewijs-hash. Een statusroute is geen bewijs dat het gemelde werk zelf is uitgevoerd.
-

Veiligheid

- Exact één actieve eigenaar per rol.
 - `max_answers=1` , `hop_count=0` , relay- plus lokale deduplicatie.
 - Harde cap: vijf Buzz-calls per run.
 - Sleutel alleen uit Keychain; niet in bestanden of logs. Keychain en Buzz worden via vaste absolute systeempaden gestart en de Buzz-child krijgt alleen vier noodzakelijke omgevingsvelden.
 - Geen klant-, salon-, mailbox- of schooldata in de proef.
 - Agents schrijven niet in elkaars werkmap.
-

Veilige neutrale statusbrug

De brug gebruikt één neutrale route:

1. Vier identity-labelled synthetische fixtures met de labels Codex, Claude, Kimi en Hermes zijn naar de afgeschermdde inbox gestaged. Dit waren geen live agent-turns en de labels zijn geen cryptografisch auteursbewijs.
2. De launchd-daemon `n1.haarvisie.agent-status-bridge` valideerde, deduplicateerde en schreef naar het canonieke register. `submit` stageert alleen; alleen deze daemon routeert naar Buzz en de cockpit. De daemon start via `env -i` , zodat geërfde procesvariabelen niet worden meegenomen.
3. De lokaal gesimuleerde workspace-hookcode bood alle vier event-id's aan als korte, alleen-lezen context voor Antigravity.

4. Een synthetische Antigravity-fixture is daarna teruggestaged. De finale v2 is `AGY_BRIDGE_E2E_20260928_02` .
5. De Codex/Claude- en Kimi-start-hookcodepaden lazen de feed terug. Hermes is in de live desktop-UI teruggelezen. Dit zijn geen live Codex-, Claude- of Kimi-modelturns.

De Buzz-controle vond voor de v2-fixture **exact één** statusbericht op basis van `event_id=AGY_BRIDGE_E2E_20260928_02` . Het gesigioneerde Buzz-event is `1f02102cc8fdd4a65aa641cf672209eb3c481c49518ed56f5b253b0804dc47f9` .

De herhaling gaf:

- `processed=0`
- `duplicates=1`
- `forwarded=0`
- `pending_buzz=0`

De openbare feed bevat uitsluitend enums, ids, tijden en hashes. Elke regel draagt `source_assurance=unverified_local_claim` ; toegestane herkomst is alleen `fixture` of `local_drop_unverified` . Vrije samenvattingen en vervolgstappen gaan niet mee.

Dit bewijst de fixture-route, automatische daemonroute en deduplicatie. Het bewijst nog niet dat

Antigravity Desktop de workspace-hook zelf heeft uitgevoerd. De simulatie meldde daarom expliciet `actual_antigravity_invocation_claimed=false` .

De resterende first-party stap is klein en datavrij: open deze workspace in Antigravity, controleer of `neutral-agent-status-feed` onder `Settings > Customizations > Hooks` staat en voer één normale datavrije beurt uit. Deze controle gebeurt handmatig in de first-party app, niet via CLI, CUA, ACP of modelautomatisering.

Upstream grens en lokale overbrugging

Hermes

De ingebouwde Buzz ACP-keten publiceert gestreamde Hermes-antwoorden nog niet. Dit is upstream Buzz-bug #4923; de herstel-PR #7249 staat nog open. De lokale route gebruikt daarom één beperkte MCP-tool. Die kan alleen antwoorden op een door de eigenaar ondertekend bericht dat Hermes exact adresseert in het vaste proefkanaal. De tool haalt de agentsleutel zelf uit Keychain en toont hem niet aan Hermes.

Bewijs: prompt `5a4b68ad...` gaf exact één gesigneerde Hermes-reply `e6afda04...` . Een herhaling gaf `already_published` en geen tweede bericht.

Antigravity/Gemini

Antigravity 2.17.0 heeft lokaal een geldige bestaande sessie. De officiële Antigravity CLI 1.2.12 hergebruikte die sessie in één datavrije proef en gaf exact `ANTIGRAVITY_LOCAL_OK` ; er zijn geen tools of werkbestanden gebruikt. Daarnaast publiceert Google `antigravity-acp` 1.2.1 via het officiële ACP-register. Buzz 0.5.25 kan die server technisch als custom harness starten.

Dat is toch niet via Buzz uitgevoerd. Antigravity Terms §6 zegt dat toegang via software, tools of diensten van derden een schending is. De officiële FAQ bevestigt dit, noemt mogelijke accountschorsing en verwijst third-party agents naar Gemini Enterprise of een Google AI Studio API-key. Buzz is software van een derde.

De technische route is dus gevonden, maar de persoonlijke OAuth-route is een harde voorwaardenblokkade. Er is geen Buzz-agent aangemaakt, geen nieuwe login gestart en geen betaalde route gebruikt. De neutrale statusbrug omzeilt deze grens niet: zij deelt alleen een korte statusfeed via de officiële workspace-hook en gebruikt geen Antigravity-model via Buzz. Een modelkoppeling via Buzz blijft alleen mogelijk na schriftelijke Google-bevestiging, of na Jamals expliciete keuze voor een Enterprise/API-keyroute met mogelijke kosten.

Bestanden

- `buzz_router.py` — router en remmen.
- `hermes_buzz_reply_mcp.py` — beperkte Keychain-backed Hermes-replytool.

- `agent-register.json` — eigenaarschap, profielen en bewezen status.
- `activity-log.jsonl` — append-only auditlog.
- `ROUTER-ONTWERP.md` — protocol en acceptatiebewijs.
- `HERMES-COCKPIT-INTEGRATIE.md` — live cockpitkoppeling en rollback.
- `ANTIGRAVITY-BUZZ-BEWIJS-2026-09-28.md` — technische route, lokaal bewijs en voorwaardenblokkade.
- `STATUS-BRIDGE-OPERATIONEEL-BEWIJS.json` — finale fixture-E2E, automatische daemonroute, deduplicatie, consumer-readback en de nog open first-party Antigravity-stap.