

Offsite backup outcome-gate popravke — MC #107366

Offsite backup outcome-gate popravke — MC #107366

Datum closeouta: 2026-08-21
Komponenta: `boot.sh`, `daemons/offsite-backup.sh`, `tools/alert-gate.js`
Canonical commit: `20f29d7c6463a3d7169dcbf050c3d0071b84a969`
Build/validation: Fusion Harness — Opus 5 high acceptance gate + GPT-5.6 Sol high builder
Nezavisni peer: Claude Sonnet — PASS, P0=0/P1=0

Problem

Backup monitoring je imao četiri povezana defekta koji su mjerili tekst umjesto ishoda:

1. Boot je čitao drugi log od onoga u koji daemon piše.
2. Riječ `Error` unutar uspješnog `Errors: 0` sažetka davala je lažni kvar.
3. Storage-cap provjera je pretraživala cijeli append-only log. Jedna stara cap greška zato je svaki kasniji kvar pogrešno pretvarala u benigni cap verdict i exit 0.
4. Alert gate ostajao je trajno `escalated` i poslije uspješnog oporavka. Budući stvarni kvar zato je mogao biti utišan.

D1/D2 — boot ?ita pravi ishod

`boot.sh` sada čita `logs/offsite-backup.log` i parsira zadnji strukturirani sažetak:

Total targets: N | Success: N | Failed: N

Verdict zavisi od numeričkog `Failed`, ne od podniske `Error`. Testovi potvrđuju:

- `Failed: 0` uz prisutne riječi `Errors: 0` → `OK`

- pozitivan `Failed` → `FAIL:N`

D3 — cap provjera samo nad tekućim runom

Daemon na početku pamti byte offset loga. Cap detekcija čita samo sadržaj dodat u trenutnom runu:

```
LOG_START_OFFSET + tail -c
```

Dokaz oba smjera:

- stara cap greška + trenutni generički kvar → `PARTIAL FAILURE`, exit 1
- stvarni trenutni `storage_cap_exceeded` → cap grana, exit 0 radi sprečavanja watchdog restart petlje

Stvarni run 20.08. u 16:12 bio je pravi trenutni B2 cap događaj: 5/9 uspješno, 4/9 palo. Nije bio historijski lažni pozitiv.

D4 — uspješan recovery ?isti stale escalation

Preostali živi kvar pronađen je tokom closeouta: više uspješnih 9/9 runova nije očistilo `com.john.offsite-backup` escalation, pa je alert gate i dalje vraćao `SUPPRESSED`.

Popravka:

- samo uspješna `fail_count == 0` grana poziva `alert-gate.js clear com.john.offsite-backup`;
- clear se izvršava prije OK Slack poruke;
- ako clear statea ne uspije, run pada zatvoreno s exit 1 i ne javlja lažni healthy recovery;
- cap i non-cap failure grane nikada ne čiste escalation;
- produkcijski alert-state path ostaje `/tmp/ops-alert-state.json`;
- dodan je backward-compatible `OPS_ALERT_STATE_FILE` override isključivo za hermetične testove.

Testovi

Novi offline test `tests/alert-recovery-107366.test.js` koristi disposable HOME, fake rclone/Slack/sqlite/perl i privremeni alert state. Ne kontaktira B2, Slack ni cloud.

```
7 tests
7 pass
0 fail
```

Pokriveno:

- escalation suppresses dok je aktivan;
- success ga čisti;
- naredni stvarni kvar ponovo može alertirati;
- 60-minutna duplicate suppression ostaje;
- historijski cap ne kontaminira trenutni non-cap kvar;
- trenutni pravi cap ostaje posebna grana;
- boot status u oba smjera.

Nezavisni peer dodatno je mutirao D3 i D4 nazad u pokvareno stanje; testovi su oba puta pali kako se očekuje. Peer verdict: PASS, P0=0/P1=0.

Live ishod

Nakon ranijeg cap događaja slijedili su uspješni stvarni runovi:

```
20.08. 22:14 – 9/9
21.08. 04:15 – 9/9
21.08. 10:16 – 9/9
21.08. 16:17 – 9/9, 0 failed
```

Poslije canonical commita ručno je očišćen samo stale key za `com.john.offsite-backup`:

```
CLEARED: com.john.offsite-backup – alerts re-enabled
ALLOWED: com.john.offsite-backup can alert
```

Ostali service state zapisi ostali su semantički identični. Sljedeći uspješan daemon run sada ovo radi automatski.

Evidence

- `/Users/makinja/system/evidence/107366/findings-2026-08-19.md`

- `/Users/makinja/system/.claude/worktrees/flowforge-107018/evidence/107366/report-2026-08-21.md`
- `/Users/makinja/system/evidence/107366/peer-validator-claude-sonnet-2026-08-21.md`
- `/Users/makinja/system/evidence/107366/live-alert-recovery-clear-2026-08-21.md`
- `/tmp/fusion-harness-eNGP2o/summary.json`

Rollback

```
cd /Users/makinja/system
git revert 20f29d7c6463a3d7169dcbf050c3d0071b84a969
```

Ako se rollback uradi, stale alert state više se neće automatski čistiti nakon recoveryja.

Van scopea

- Alert-gate shared-state read/modify/write nema cross-process lock; to je pre-existing race rizik i kandidat za zaseban task.
- B2 storage cap je stvaran kapacitetni događaj, ne kodni kvar ove popravke.
- `.bookstack-cred-cache.json` i drugi credential-cache artefakti u backup scopeu ostaju zasebno pitanje higijene.

Revision #1

Created 2026-08-21 14:54:54 UTC by John

Updated 2026-08-21 14:54:54 UTC by John