

# Runtime DB rola bez BYPASSRLS — preduslov #1 RLS lanca (MC #900174)

# Runtime DB rola bez BYPASSRLS — preduslov #1 RLS lanca (MC #900174)

**Izvor:** MC #900154 NO-GO audit + živa potvrda (`~/system/evidence/900154/runtime-role-live-probe-20260823.md`): `bilko-api-demo` se konektuje kao `DATABASE_USER=bilko_admin` (BYPASSRLS, V30\_1/V32) → Postgres ne evaluira RLS ni u kom modu; jedina živa izolacija je aplikacioni `WHERE org_id`.

## Scope

- Nova ne-bypass runtime rola (npr. `bilko_app`) + GRANT-ovi nad app tabelama/sekvencama (migracija).
- `DATABASE_USER` promjena na **demo prvo**; stage/prod poslije soak metrika (#900154).
- Flyway korisnik (`bilko_admin`) se NE dira.
- PRIJE dizajna GRANT-ova: deciding-fact upit iz #106342 (`SELECT rolname, rolbypassrls FROM pg_roles WHERE rolname='bilko_admin'` na demo/stage/prod) — mijenja pretpostavke.
- Ceremonija: puni H put — /prompt-forge → /mehanik → builder worktree → nezavisni verifier → soak.

## Acceptance

- ☐ `pg_roles` dokaz: nova rola bez `rolbypassrls`
- ☐ API smoke svi CRUD tokovi zeleni s novom rolom na demo
- ☐ RLS se evaluira: upit bez `app.current_org_id` pod novom rolom na FORCE-RLS tabeli → 0 redova

☐ Rollback dokumentovan i testiran (vratiti DATABASE\_USER)

☐ Soak metrike definisane prije stage/prod promocije

---

Revision #3

Created 2026-08-23 18:08:33 UTC by John

Updated 2026-08-23 18:09:20 UTC by John