

# Bilko support repo split — plan (2026-08-23)

## MC #900161 — Plan: izdvajanje bilko.cloud support surface u novi AzDO repo

CEO nalog: "kao sto smo izvukli image, container treba src code i pipeline izvuci — dva projekta main/support." Ovo je PLAN, ne implementacija. Čeka CEO odobrenje prije bilo kakvog reza u kodu ili pipeline-u.

### 1. Cilj

Nezavisan support lifecycle: deploy supporta ne čeka main CI, main incident ne blokira support fix. Čišća RBAC/blast-radius granica — support je admin-only površina, danas dijeli sliku i deploy rizik s main-om. Krajnji rezultat: support.bilko.cloud servira se iz vlastitog repoa/pipeline-a/slike, main repo ostaje netaknut.

### 2. Stanje danas (izvor: scout-pipeline.md, scout-code.md)

- Support nema vlastiti build/scan: jaše na main-ovom `build_demo_web` jobu (azure-pipelines.yml:2166-2195), ista `apps/web/Dockerfile`, isti tag `bilko-web:demo-${SHORT_SHA}`, isti ACR `bilkodemo.azurecr.io`.
- Deploy je jedini support-specifičan korak: 2. `az containerapp update` (2309-2320) na `bilko-web-support-demo`, postavlja `BILKO_APP_SURFACE=support` kao runtime env var (nije build ARG — ista slika, dva poda).
- Verify: 3 curl provjere (2376-2408): `/admin` → 307, `/dashboard` → 404, `/invoices` → 404 na support.bilko.cloud.

- Kod: 8 support-only fajlova pod `app/(admin)/admin/*`, 12 dijeljenih auth fajlova (8 lib + 4 stranice), 6 backend endpointa pod `/admin/*` namespace-om, 30 testova u `app-surface-900075.test.ts`. Ukupno ~35-40 fajlova za novi repo (scout-code.md summary tabela).
- Support postoji SAMO na demo tier-u — nula footprint u `CI_Gates/Build/Deploy_Stage/E2E_UAT/Write_UAT`.

### 3. Odluka za CEO #1 — isti AzDO projekat (novi repo) vs novi AzDO projekat

Kelsey (pipeline scout) preporučuje: **novi REPO u postojećem Bilko projektu**, ne novi projekat.

- Agent pool (bilko-selfhosted, 1 org-wide CI slot) je org-level resurs — dijeli se identično bez obzira na odluku.
- Service connection `azure-bilko` i variable group `bilko-kv-demo` (Key Vault-linked) su project-scoped po defaultu. Novi projekat = ponovno kreiranje/grant SP permisija i dupliranje variable grupa. Novi repo u istom projektu nasljeđuje sve to plus postojeći `Promote_Demo` environment approval gate, bez dodatnog AzDO admin posla. **Pitanje za CEO-a:** kad kažeš "dva projekta", misliš li na RBAC/board izolaciju (support tim ne vidi main backlog/work items) ili na tehničku separaciju build/deploy lanaca? Ako je prvo — novi projekat ima smisla uprkos trošku re-provisioninga. Ako je drugo (isporuka/rizik razdvojeni) — repo u istom projektu postiže isti tehnički cilj bez ponovnog AzDO admin rada. **Moja preporuka:** repo u istom projektu, osim ako je RBAC izolacija eksplicitan zahtjev — tehnički cilj (nezavisan lifecycle) se postiže repoom i pipeline-om, ne granicom projekta.

### 4. Odluka za CEO #2 — dijeljeni auth kod (12 fajlova) i API klijent

Dvije opcije: (a) git subtree pull pinovan na main-ov SHA, ponovna sinhronizacija ručnim korakom; (b) zajednički npm paket (interni registry/workspace), verzionisan i publikovan. Kelsey upozorava: "pin, ne copy-paste, protiv tihog drifta" — čisti copy-paste bez pina je isti obrazac koji je već izazvao tihi drift na drugim mjestima (RS mali preduzetnik, HR kontni plan — vidi memoriju). **Moja preporuka za mali tim (1 čovjek + AI agenti održava oba repoa):** git subtree, pinovan na eksplicitan main SHA, dokumentovan ručni resync postupak. Zajednički paket je arhitektonski čišći dugoročno, ali dodaje publish pipeline + registry — novi CI surface koji troši isti org-wide slot i nije opravdan za 12 fajlova koji se rijetko mijenjaju (MSAL/auth integracija je stabilna, ne sedmični churn). Eksplicitan SHA pin čini drift vidljivim i revizibilnim umjesto nevidljivim.

## 5. Faze

### F1 — novi repo + pipeline skeleton + fork slike + paralelni test pod (main repo se NE dira)

1. Kreirati novi AzDO repo (`bilko-web-support`) u Bilko projektu (per odluka #1).
2. Skeleton `azure-pipelines.yml`: stage `Build_Scan` — vlastiti Dockerfile, build+push `bilko-web-support:${SHORT_SHA}` u isti ACR.
3. Registrovati/ponovo iskoristiti `SC_AZURE` service connection, ACR push pristup, variable group (slimana `bilko-kv-demo` podskupina).
4. Vlastiti Trivy image scan (HIGH,CRITICAL) — danas se "vozi" na main-ovom skenu iste slike, ta pokrivenost nestaje čim se slika forkuje ako se ne duplira.
5. Stage `Deploy_Support_Demo`: deploy na NOVI test ACA pod (`bilko-web-support-demo-v2`) — postojeći `bilko-web-support-demo` ostaje netaknut.
6. Stage `Verify`: 3 PI2-ekvivalentne provjere protiv v2-ovog direktnog ACA FQDN-a (ne custom domain).
7. Potvrda: main repo `azure-pipelines.yml` diff = 0 linija. **Trajanje:** 6-10h agentskog rada (pipeline skeleton, AzDO wiring, paralelni pod, verify). **Izlazni kriterij:** v2 pod ispravno odgovara na 3 provjere na direktnom FQDN-u, scan prolazi, main pipeline netaknut.

### F2 (tek poslije CEO odobrenja) — src ekstrakcija + testovi + cutover

1. Ekstrakcija 8 support-only fajlova (`app/(admin)/admin/*`).
2. Ekstrakcija/subtree-pin dijeljenog auth sloja (12 fajlova) na izabran main SHA (odluka #2).
3. Ekstrakcija core mehanizma: `app-surface.ts`, `middleware.ts`.
4. Migracija `lib/api.ts` admin metoda (6 endpointa: listOrgs, getOrg, patchOrg, listOrgUsers, impersonate, endImpersonation).
5. Migracija/adaptacija `app-surface-900075.test.ts` (30 testova) u CI novog repoa; odlučiti da li ostaje i u main repou (boundary logika za `/` ostaje relevantna glavnoj aplikaciji do F3).
6. Ožičenje env varijabli (7 `NEXT_PUBLIC_*` + `BILKO_APP_SURFACE=support` kao ACA runtime env, ne build ARG).
7. Cutover: repoint custom-domain binding `support.bilko.cloud` → v2 target (isti managed-cert obrazac kao MC #105793) — DNS se ne dira, samo ingress binding target.
8. Soak prozor na starom podu (ostaje živ, ne briše se) — rollback = repoint binding nazad, bez rebuilda. **Trajanje:** 14-20h agentskog rada (najveći komad: paritet testova + potvrda da `platformAdmin` JWT i dalje radi kroz novi build). **Izlazni kriterij:** support.bilko.cloud servira novi pod, 3 PI2 provjere + 30 testova zeleni na novom repou, soak prozor (preporuka 48-72h) prošao bez incidenta, stari pod i dalje živ.

# F3 (tek poslije F2 soak-a) — ?iš?enje main repoa

1. Ukloniti support deploy/verify blokove iz `azure-pipelines.yml` (2309-2320, 2376-2408).
  2. Ugasiti stari `bilko-web-support-demo` pod.
  3. Ukloniti support-only kod iz `apps/web` (`app/(admin)/*`, `BILKO_APP_SURFACE` gating) nakon potvrde da main više ne referencira.
  4. Odlučiti sudbinu `app-surface-900075.test.ts` u main CI (zadržati ako main i dalje ima admin-adjacent putanje koje test pokriva).
  5. Ažurirati BookStack runbook stranice koje referenciraju support deploy u main pipeline-u.
- Trajanje:** 3-5h. **Izlazni kriterij:** main `azure-pipelines.yml` ima nula support-specifičnih koraka, CI runtime main-a nepromijenjen.

## 6. Rizici i rollback

1. Entra redirectUri: `NEXT_PUBLIC_ENTRA_REDIRECT_URI` nije postavljen ni danas — obje površine koriste bare-origin fallback; support.bilko.cloud mora ostati u allowlisti, guard mora dozvoliti auth povratne putanje (memorija: surface guard mora dozvoliti auth redirect). Provjeriti na v2 test podu PRIJE cutovera.
2. Image drift vs main API kontrakt: nakon forka slike, support repo mora pinovati API kontrakt (docs/backend/API-REFERENCE.md ili OpenAPI artefakt) na main-API SHA — ne ručno kopirati, inače tihi drift.
3. 1 CI slot je org-wide bez obzira na odluku #1; novi pipeline NE smije otimati slot main-u — isti trigger obrazac kao main (branch-scoped, ne svaki commit/PR).
4. Trivy scan pokrivenost nestaje čim se slika forkuje ako F1 korak 4 nije tvrd izlazni kriterij, ne "nice to have".
5. Rollback mreža postoji SAMO dok stari pod živi — ako se F3 (brisanje starog poda + čišćenje main pipeline-a) izvede prije nego soak prozor iz F2 prođe, nema mreže za povratak.

## 7. Šta se ne dira

- `azure-pipelines.yml` u main repou (nula izmjena do F2 koraka 7 / F3).
- Service connections, ACR, variable group `bilko-kv-demo`, DNS zapis za support.bilko.cloud (mijenja se samo ingress binding target u F2 koraku 7, ne sam DNS zapis).
- Izvorni kod u `apps/web` monorepou ostaje nepromijenjen do F2/F3 ekstrakcije.

## 8. Procjena

| Faza                                                                                                                                                                                        | Sati agentskog rada | Šta CEO mora obezbijediti                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------|
| F1                                                                                                                                                                                          | 6-10h               | Odluka #1 i #2 prije starta; ako odluka #1 = novi projekat, treba org-admin za kreiranje projekta (agent nema tu permisiju) |
| F2                                                                                                                                                                                          | 14-20h              | Odobrenje plana (ovaj dokument) prije starta; ako odluka #1 = novi projekat, ponovni grant SP/service connection permisija  |
| F3                                                                                                                                                                                          | 3-5h                | Odobrenje da je soak prozor (48-72h) prošao                                                                                 |
| <b>Ukupno: ~23-35h agentskog rada kroz sve tri faze</b> , plus jedan ili dva administrativna CEO koraka (odluke #1/#2, eventualno AzDO project-create permisija ako se bira novi projekat). |                     |                                                                                                                             |

# AFTER — F1 isporu?en 2026-08-24 (MC #900162)

Repo `Bilko-Support` kreiran ručno (CEO, 24.08.) nakon PAT 401 blokade od 23.08. F1 koraci 2-7 isporučeni i nezavisno verifikovani:

- Pipeline skeleton na origin/main (commit a4e0662): trigger samo main, pr none, bez schedules, Build\_Scan gated-off do F2, Trivy uvijek on, Deploy\_Support\_Demo + Verify protiv v2.
- Fork slike: `az acr import` → `bilko-web-support:demo-1d58cbb6`, digest bajt-identičan izvoru (sha256:f1002bd2...0178f).
- Trivy (FORGE): 0 HIGH/CRITICAL, exit 0.
- Novi test pod `bilko-web-support-demo-v2` Running, samo direktni ACA FQDN; verify 3/3 (/admin→307, /dashboard→404, /invoices→404).
- Main repo i stari pod netaknuti (git status baseline + lastModifiedAt identičan; customDomains nepromijenjen).
- Peer-verify (writer≠verifier): verifier-900162, Verdict PASS/VERIFIED — /Users/makinja/system/evidence/900162/peer-verify-transcript-20260824.md
- Builder evidence: /Users/makinja/system/evidence/900162/resume-report-20260824.md

Otvoreno za F2: registracija AzDO pipeline definition objekta (yml dormantan do tada); repo-id diskrepanca (c50cad02 vs c170e706) zapisana.