

MC 900210 — clamd za demo-stage upload (2026-08-24)

MC #900210 — Demo/stage bez clamd: upload karantin fail-closed (2026-08-24)

Task: [Bilko][H][UPLOAD] Demo/stage nemaju clamd — svaki upload SCAN_FAILED→karantin; CEO blokirao na re-testu #900178.

Nalaz (mašinski dokaz, 2026-08-24 18:44Z)

- LogAnalytics (ContainerAppConsoleLogs_CL, bilko-api-demo): ClamAvScanner scan I/O error against localhost:3310 – Connection refused → ReceiptService REJECTED – SCAN_FAILED_QUARANTINED (fail-closed), inbox 10e5aa86.
- **Gate radi tačno po dizajnu** (UploadSecurityGate, G1-02/#106852): INFECTED i SCAN_FAILED → QUARANTINED, nikad release. Kvar je što demo/stage **nemaju clamd servis**: 1 kontejner po appu, 0 CLAMD_* env varova (verifikovano az query-jem). CI je zelen jer Testcontainers diže pravi ClamAV.
- Spec docs/backend/EXTERNAL-SERVICES.md §7: clamd na localhost:3310, Docker image.
- CEO-ov fajl NIJE izgubljen — karantin zapis; re-upload poslije fixa.

Plan (najuži sankcionisani put — hard-blocker isporuke #900178)

1. Novi ACA app bilko-clamd u bilko-demo-env (rg-bilko-demo): clamav/clamav official image, internal TCP ingress exposedPort 3310, 1 CPU / 2Gi, min 1 replika.

2. `CLAMD_HOST=<interni FQDN>` na `bilko-api-demo` i `bilko-api-stage` (`--set-env-vars` je merge — preživljava pipeline deploy bez izmjene `azure-pipelines.yml`).
3. Traffic shift na novu reviziju + potvrda (`ingress traffic show`) — lekcija #105368/ACA.
4. Dvosmjerni kanarinac na živom demo-u: čist PDF → CLEAN/stored; EICAR string → `MALWARE_DETECTED` karantin. Oba smjera obavezna.
5. Rollback put: `az containerapp update --remove-env-vars CLAMD_HOST` + traffic revert (dokazan obrazac iz #900174 D5).

Evidence: `~/system/evidence/900210/`.

Revision #1

Created 2026-08-24 19:00:04 UTC by John

Updated 2026-08-24 19:00:04 UTC by John