

# QODY Infra Reconciliation — Session d342b20a (demo/prod split, DNS, firewall, CORS)

## QODY Infra Reconciliation — Session d342b20a (2026-06- 28/29)

**Type:** Post-session infra reconciliation (ZAKON DOC) **Source session:** d342b20a-e460-4153-8423-7586072b73ae (John, 2026-06-28 to 2026-06-29) **Written by:** FlowForge (2026-06-30) **Status:** READ-ONLY record — no infrastructure mutations applied here.

---

## What This Session Did

Session d342b20a executed approximately 34 infrastructure operations across two days (2026-06-28 and 2026-06-29) covering: PostgreSQL firewall rules, ACA env-var updates (CORS\_ORIGINS + APP\_BASE\_URL), Cloudflare DNS records on the qody.ba zone, and a Cloudflare Pages landing deployment. It also opened 9 MC follow-up tasks.

---

## Environment Topology (Verified 2026-06-30)

QODY runs two fully separate environments sharing one Azure subscription.

Production — rg-qody-prod

| Component           | Value                                                              |
|---------------------|--------------------------------------------------------------------|
| Resource group      | rg-qody-prod                                                       |
| ACA environment     | gentlecliff-98883162 (swedencentral)                               |
| Container registry  | qodyprodacr.azurecr.io                                             |
| PostgreSQL          | qody-prod-db.postgres.database.azure.com<br>(Standard_B1ms, PG 16) |
| API app             | qody-api-prod                                                      |
| Guest MFE           | qody-guest-prod                                                    |
| Admin MFE           | qody-admin-prod                                                    |
| Kitchen MFE         | qody-staff-kitchen-prod                                            |
| Custom domains      | api.qody.ba / app.qody.ba / admin.qody.ba /<br>kuhinja.qody.ba     |
| TLS                 | Azure-managed (Let's Encrypt, SNI, per-app cert)                   |
| Seed                | None — clean prod DB, DEMO_SEED_ENABLED=false, ENV=prod            |
| Status (2026-06-30) | LIVE — Phase C cutover complete (DEPLOY-MAP v1.6.0)                |

## Demo/Stage — rg-qody-demo

| Component             | Value                                                                   |
|-----------------------|-------------------------------------------------------------------------|
| Resource group        | rg-qody-demo                                                            |
| ACA environment       | blueplant-5a0ce6b3 (swedencentral)                                      |
| Container registry    | qodydemoacr.azurecr.io                                                  |
| PostgreSQL            | qody-demo-db.postgres.database.azure.com<br>(Standard_B1ms, PG 16)      |
| API app               | qody-api                                                                |
| Guest MFE             | qody-guest                                                              |
| Admin MFE             | qody-admin                                                              |
| Kitchen MFE           | qody-staff-kitchen                                                      |
| Primary demo domain   | qody.alai.no + api/admin/kuhinja.qody.alai.no                           |
| Secondary demo domain | demo.app/demo.api/demo.admin/demo.kuhinja.qody.ba                       |
| TLS                   | Azure-managed (Let's Encrypt)                                           |
| Seed                  | Full demo venue "QODY Demo Bistro" (V7 idempotent),<br>Stripe test mode |
| Status (2026-06-30)   | LIVE                                                                    |

# Landing Page — Cloudflare Pages (Edge)

| Component           | Value                                                    |
|---------------------|----------------------------------------------------------|
| CF Pages project    | qody-landing                                             |
| CF account          | SnowIT (d0ac2afb6bb5b298723b85a114151a04)                |
| Source dir          | apps/landing/ (no build step; deploy dir directly)       |
| Deploy token        | Bitwarden "Cloudflare API Token — alai-web Pages Deploy" |
| Custom domains      | qody.ba, www.qody.ba                                     |
| Status (2026-06-30) | LIVE                                                     |

## CORS\_ORIGINS and APP\_BASE\_URL — Final Verified Values (2026-06-30)

These values were queried live from Azure (`az containerapp show`) and represent the actual current state of the two API containers.

### qody-api (demo, rg-qody-demo)

```
CORS_ORIGINS =  
https://demo.app.qody.ba,https://demo.admin.qody.ba,https://demo.kuhinja.qody.ba  
APP_BASE_URL = https://demo.app.qody.ba
```

**Gap identified:** `qody.alai.no`, `admin.qody.alai.no`, and `kuhinja.qody.alai.no` are NOT in CORS\_ORIGINS. These DNS names still point to the demo ACA apps (dig-verified). Any browser loading the guest MFE from `https://qody.alai.no` will have its API calls to `demo.api.qody.ba` rejected by CORS (Origin header mismatch). The earlier transcript shows the session did set a broader value that included `qody.alai.no` origins, but the final state was narrowed to `demo*.qody.ba` only. This should be reconciled by either: (a) adding `https://qody.alai.no,https://admin.qody.alai.no,https://kuhinja.qody.alai.no` back to CORS\_ORIGINS on qody-api; or (b) removing the DNS entries for *.qody.alai.no* and relying exclusively on *demo..qody.ba*. The DEPLOY-MAP v1.6.0 lists both sets of demo domains as active, so option (a) is the correct fix.

### qody-api-prod (production, rg-qody-prod)

```
CORS_ORIGINS = https://app.qody.ba,https://admin.qody.ba,https://kuhinja.qody.ba,
               https://qody-guest-prod.gentlecliff-
98883162.swedencentral.azurecontainerapps.io,
               https://qody-admin-prod.gentlecliff-
98883162.swedencentral.azurecontainerapps.io,
               https://qody-staff-kitchen-prod.gentlecliff-
98883162.swedencentral.azurecontainerapps.io
APP_BASE_URL  = https://qody-guest-prod.gentlecliff-
98883162.swedencentral.azurecontainerapps.io
```

**Gap identified:** `APP_BASE_URL` on the prod API is still the raw ACA FQDN, not the custom domain `https://app.qody.ba`. This matters for receipt email links — they will contain the raw ACA URL instead of the branded domain. Should be updated to `https://app.qody.ba`. The `CORS_ORIGINS` already includes the custom domains so that path is correct; the ACA FQDNs in `CORS_ORIGINS` are redundant but harmless.

## Firewall Rules — Current State (2026-06-30, verified via az)

### qody-prod-db (rg-qody-prod)

| Rule name                                                                       | Start IP      | End IP        | Status                                     |
|---------------------------------------------------------------------------------|---------------|---------------|--------------------------------------------|
| <code>temp-bootstrap-1782738781</code>                                          | 92.221.168.61 | 92.221.168.61 | TEMP — delete after CEO bootstrap complete |
| <code>allow-anvil</code>                                                        | 92.221.168.61 | 92.221.168.61 | Labeled permanent; same ANVIL host IP      |
| <code>AllowAllAzureServicesAndResourcesWithinAzureIps_2026-6-23_17-41-11</code> | 0.0.0.0       | 0.0.0.0       | Standard Azure-services rule (OK)          |
| <code>temp-bootstrap-1782738848</code>                                          | 92.221.168.61 | 92.221.168.61 | TEMP duplicate — delete                    |

**Recommendation:** Delete `temp-bootstrap-1782738781` and `temp-bootstrap-1782738848` (duplicates of `allow-anvil`). Retain `allow-anvil` and the Azure-services rule. The session comment was "DELETE after CEO bootstrap" — CEO has had time to bootstrap; these rules should now be cleaned up. Confirm with CEO/FlowForge before deleting.

### qody-demo-db (rg-qody-demo)

| Rule name                   | Start IP      | End IP          | Status                              |
|-----------------------------|---------------|-----------------|-------------------------------------|
| temp-repair-1782739048      | 92.221.168.61 | 92.221.168.61   | TEMP — delete after repair complete |
| AllowAll_2026-6-22_22-42-10 | 0.0.0.0       | 255.255.255.255 | <b>RISK: entire internet</b>        |
| temp-repair-1782738983      | 92.221.168.61 | 92.221.168.61   | TEMP duplicate — delete             |

**High-severity risk:** AllowAll\_2026-6-22\_22-42-10 (0.0.0.0 to 255.255.255.255) opens the demo Postgres flexible server to the entire internet. This rule predates session d342b20a (created 2026-06-22). It was not added by this session and was not removed by this session. Protection relies entirely on username/password credentials and SSL enforcement. Recommended action: replace with a narrower rule set (ANVIL IP + Azure-services 0.0.0.0/0 rule) to reduce attack surface. Demo data is not production PII, but the broad rule is an unnecessary exposure.

The two temp-repair rules for 92.221.168.61 were added by this session for schema repair operations and can now be deleted.

# DNS State — qody.ba Zone (2026-06-30, verified via dig)

DNS is managed in Cloudflare zone 4b8701ed4f2bd0133cd561ee20d7a30f in SnowIT account d0ac2afb. Session d342b20a added the demo subdomain records (demo.\*.qody.ba) and the asuid TXT verification records via the Cloudflare API.

## Production records (added before or during session)

| Host          | Type  | Target                                                                   | Live               |
|---------------|-------|--------------------------------------------------------------------------|--------------------|
| api.qody.ba   | CNAME | qody-api-prod.gentlecliff-98883162.swedencentral.azurecontainerapps.io   | Yes (dig-verified) |
| app.qody.ba   | CNAME | qody-guest-prod.gentlecliff-98883162.swedencentral.azurecontainerapps.io | Yes (dig-verified) |
| admin.qody.ba | CNAME | qody-admin-prod.gentlecliff-98883162.swedencentral.azurecontainerapps.io | Per DEPLOY-MAP     |

| Host                  | Type  | Target                                                                           | Live               |
|-----------------------|-------|----------------------------------------------------------------------------------|--------------------|
| kuhinja.qody.ba       | CNAME | qody-staff-kitchen-prod.gentlecliff-98883162.swedencentral.azurecontainerapps.io | Per DEPLOY-MAP     |
| qody.ba               | CNAME | qody-landing.pages.dev                                                           | Per DEPLOY-MAP     |
| www.qody.ba           | CNAME | qody-landing.pages.dev                                                           | Per DEPLOY-MAP     |
| asuid.api.qody.ba     | TXT   | 908FCBD4D627093B529453581918B64EC8D7188D7D595BE1124DA8298DAC671D                 | Azure verification |
| asuid.app.qody.ba     | TXT   | (same)                                                                           | Azure verification |
| asuid.admin.qody.ba   | TXT   | (same)                                                                           | Azure verification |
| asuid.kuhinja.qody.ba | TXT   | (same)                                                                           | Azure verification |

## Demo records (added by session d342b20a via Cloudflare API)

| Host                 | Type  | Target                                                                    | Live               |
|----------------------|-------|---------------------------------------------------------------------------|--------------------|
| demo.api.qody.ba     | CNAME | qody-api.blueplant-5a0ce6b3.swedencentral.azurecontainerapps.io           | Yes (dig-verified) |
| demo.app.qody.ba     | CNAME | qody-guest.blueplant-5a0ce6b3.swedencentral.azurecontainerapps.io         | Yes (dig-verified) |
| demo.admin.qody.ba   | CNAME | qody-admin.blueplant-5a0ce6b3.swedencentral.azurecontainerapps.io         | Per DEPLOY-MAP     |
| demo.kuhinja.qody.ba | CNAME | qody-staff-kitchen.blueplant-5a0ce6b3.swedencentral.azurecontainerapps.io | Per DEPLOY-MAP     |

All Azure-managed TLS certificates for ACA custom domains were provisioned via `az containerapp hostname add` + `az containerapp hostname bind` with the managed-cert option. The asuid TXT records were required by Azure for custom domain verification.

# MC Tasks Opened by Session d342b20a

All 9 tasks were created on 2026-06-28 or 2026-06-29. Statuses are as of 2026-06-30.

| ID      | Title                                                                                              | Priority | Status                                  | Notes                                                                                    |
|---------|----------------------------------------------------------------------------------------------------|----------|-----------------------------------------|------------------------------------------------------------------------------------------|
| #104460 | QODY waiter-call: add tableLabel to WaiterCallDto (KDS shows UUID not table name)                  | L        | open                                    | Cosmetic — banner shows table UUID instead of "Sto 3"                                    |
| #104465 | Rotate exposed Azure DevOps PAT (alai-holding/QODY)                                                | M        | open                                    | PAT was printed in session tool output; rotation deferred by CEO. DO NOT print PAT here. |
| #104467 | QODY: guard against all-kitchen-items-sold-out breaking demo/guest ordering                        | M        | open                                    | Admin banner + /health WARN when 0 items available                                       |
| #104513 | QODY demo/prod domain split — Phase A+B+C (CEO approved 2026-06-29)                                | H        | closed (complete per DEPLOY-MAP v1.6.0) | Phase C prod cutover done 2026-06-29; this was the core task of the session              |
| #104514 | QODY prod-blocker: V15 (+V16-V21) inline demo-seed FK-fails on clean prod DB                       | H        | closed (fixed per DEPLOY-MAP v1.5.0)    | Migration guard fix; Flyway V14→V21 now applies cleanly on clean DB                      |
| #104523 | QODY super-admin UX: login without venueSlug + hide platform venue from merchants list             | M        | open                                    | Small backend polish; blocks clean Asmir super-admin experience                          |
| #104525 | QODY landing: "Probaj uzivo" section — demo by role (guest/admin/kitchen/super-admin)              | M        | open                                    | New landing section with 4 role cards + live demo links                                  |
| #104526 | QODY legal/compliance pack — Lexicon DRAFTS (Privacy/ToS/Cookie/ DPA, BiH+GDPR, SnowIT controller) | H        | open                                    | No legal docs exist; QODY is live and collecting user data                               |

| ID      | Title                                                                                     | Priority | Status | Notes                  |
|---------|-------------------------------------------------------------------------------------------|----------|--------|------------------------|
| #104527 | QODY admin menu UI/UX: (1) BUG delete item/category broken (2) FEATURE daily menus by day | M        | open   | Mix of bug and feature |

# Ambiguities and Risks

- CORS gap on demo (qody.alai.no not in CORS\_ORIGINS):** Browsers accessing the old `qody.alai.no` domain will receive CORS errors when the MFE calls `demo.api.qody.ba`. The MFEs were rebuilt pointing to `demo.api.qody.ba`, but DNS for `qody.alai.no` still resolves to demo ACA apps. Action: add old demo origins to CORS\_ORIGINS, OR deprecate qody.alai.no DNS entries (DEPLOY-MAP v1.6.0 lists both as active, so add them back).
- Prod APP\_BASE\_URL uses raw ACA FQDN:** Should be `https://app.qody.ba` but is currently the ACA internal FQDN. Receipt email links will have the ugly ACA URL. Low-urgency fix (SMTP not configured yet so receipts are stubs).
- Temp firewall rules not cleaned up:** Three `temp-bootstrap` / `temp-repair` rules for 92.221.168.61 remain on both Postgres servers. They are harmless but clutter. Delete after confirming CEO bootstrap of Asmir super-admin in prod is complete.
- Demo DB AllowAll rule (0.0.0.0-255.255.255.255):** Pre-existing rule, NOT from this session. Opens demo Postgres to entire internet. Should be tightened. Acceptability depends on whether demo DB contains any real user data (it should only contain seeded demo data per V7).
- PAT rotation (#104465):** Azure DevOps PAT was printed in plaintext in session tool output. CEO deferred rotation. Until rotated, the PAT in `.git/config` remote URL should be considered compromised-in-log. No action taken here per scope constraints.
- QODY has no legal documents live:** Task #104526 is open. QODY collects guest order data and payment references via Stripe. Legally exposed until Privacy Policy and ToS are live on qody.ba.

# Evidence

- CORS\_ORIGINS and APP\_BASE\_URL: live `az containerapp show` query (2026-06-30 07:57 UTC)
- Firewall rules: live `az postgres flexible-server firewall-rule list` (2026-06-30 07:57 UTC)
- DNS: live `dig` queries (2026-06-30 07:57 UTC)
- Prod API health: `curl https://api.qody.ba/health` → `{"status": "ok", "db": {"rlsRoleCheck": {"bypassRls": false, "status": "PASS"}}}` (2026-06-30 07:57 UTC)



- Demo app: `curl -I https://demo.app.qody.ba` → HTTP 200 (2026-06-30 07:57 UTC)
  - MC tasks: transcript grep + `mc.js show` (task IDs confirmed from session tool-result lines)
  - Source transcript: `~/ .claude/projects/-Users-makinja/d342b20a-e460-4153-8423-7586072b73ae.jsonl`
  - Canonical infra authority: `~/business/ALAI-Holding-AS/products/qody/DEPLOY-MAP.md` (v1.6.0, 2026-06-29)
- 

*Document authority: FlowForge. Changes to live infra require ZAKON PI2 verification. For full deployment procedures see DEPLOY-MAP.md in the QODY repo.*

---

Revision #1

Created 2026-06-30 08:01:40 UTC by John

Updated 2026-06-30 08:01:40 UTC by John