

Fő megállapítások:

✅ Működik:

- OpenClaw gateway + 10 custom skill
- SQLite adatbázisok (4 db)
- Mission Control dashboard (real-time)
- Docker Compose deployment

🔥 Kritikus problémák:

- OpenClaw dev gateway **PUBLIKUSAN elérhető** (0.0.0.0:18789) - azonnali javítás szükséges
- API kulcsok plaintext az .env fájlokban
- Duplikált architektúra (dev + navibase instance)

❌ Hiányzik a tervezett architektúrából:

- Cloudflare Tunnel
- Deploy/backup szkriptek (dokumentáció van, kód nincs)
- Telegram notifications (konfig van, de üres)
- Email értesítések

🟡 Nem tervezett, de implementált:

- ClawGuard monitoring service
- Külön Kanban service (az architektúra szerint skill-ben kellene lennie)
- Snapshot-writer külön konténer

A részletes jelentés tartalmaz:

- Current State Diagram
- Drift Report (tervezett vs. tényleges)
- Risk List (prioritizálva)
- Data flow audit
- Security audit
- Következő lépések priorizálása

NAVIBASE / OPENCLAW STACK – RENDSZER AUDIT JELENTÉS

Dátum: 2026-02-13

Környezet: /opt könyvtár (dn-dev-02)

Audit típus: Architecture drift analysis (tervezett vs. tényleges)

EXECUTIVE SUMMARY

A Navibase OpenClaw stack **részben implementált** állapotban van. Az alapvető architektúra működik (OpenClaw gateway + custom skills + Mission Control UI), de jelentős eltérések vannak a tervezett architektúrától:

✅ Működik:

- 1 agent (Főnök) + 10 custom skill
- SQLite alapú adatperzisztencia
- Mission Control dashboard (real-time)
- Docker Compose deployment
- Budget tracking + approval gate + audit log

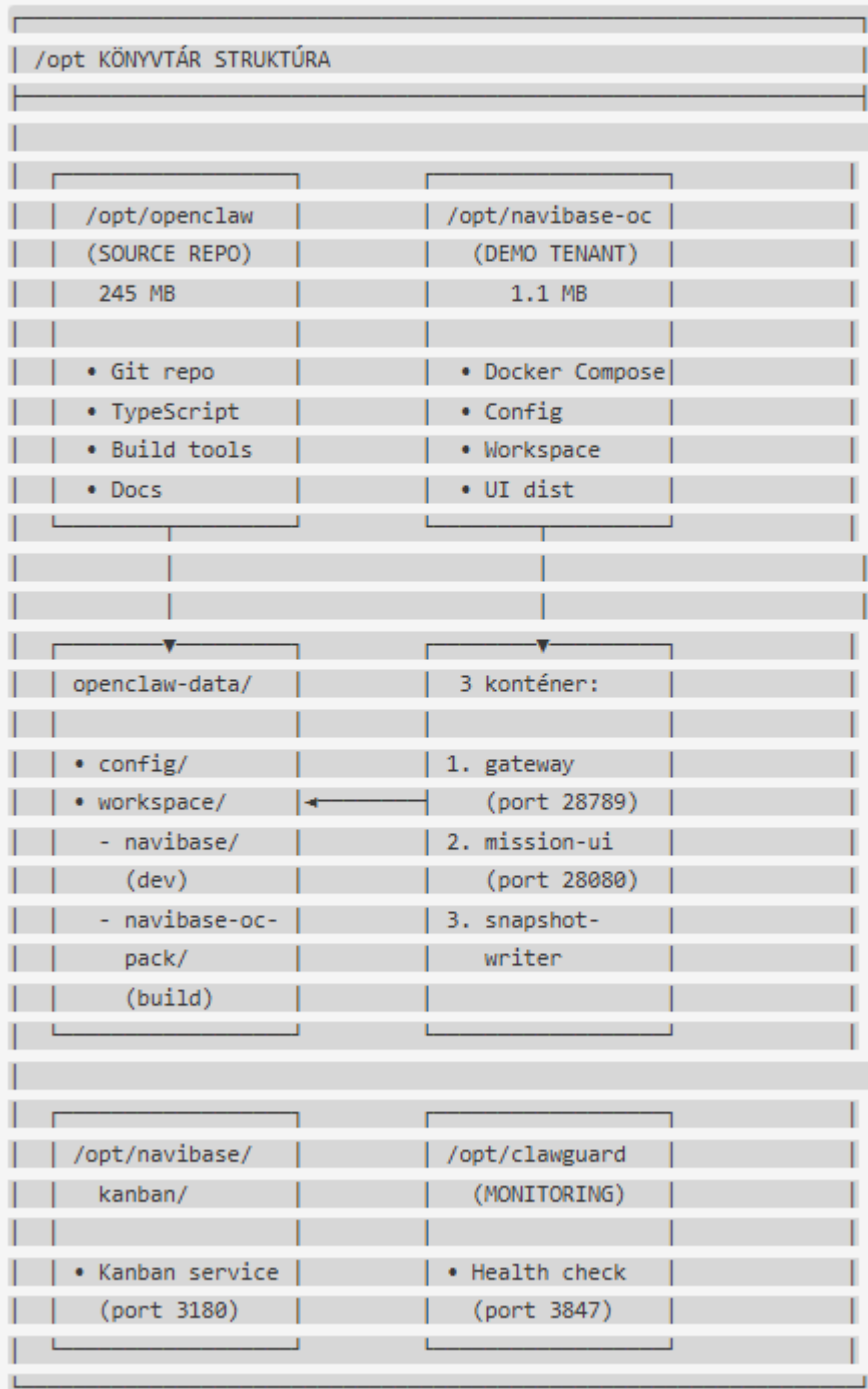
❌ Hiányzik:

- Cloudflare Tunnel
- Idempotens deploy script
- Backup/rollback rendszer
- Telegram notifications
- Dokumentált delivery flow

🚨 Kritikus problémák:

- OpenClaw dev gateway PUBLIKUSAN elérhető (0.0.0.0:18789)
- API kulcsok plaintext az .env fájlokban
- Duplikált architektúra (dev vs. navibase instance)

1. CURRENT STATE DIAGRAM



RUNTIME KONTÉNEREK:

| CONTAINER NAME | PORT BINDING | STATUS | |
|--------------------------------|------------------|--------|---|
| openclaw-openclaw-gateway-1 | 0.0.0.0:18789-90 | Up 46h | ⚠ |
| navibase-oc-openclaw-gateway | 127.0.0.1:28789 | Up 8h | ✓ |
| navibase-oc-mission-control-ui | 127.0.0.1:28080 | Up 12h | ✓ |
| navibase-oc-snapshot-writer | (none) | Up 28h | ✓ |
| navibase-kanban | 127.0.0.1:3180 | Up 4h | ✓ |
| clawguard | 127.0.0.1:3847 | Up 2d | ✓ |

DOCKER NETWORKS:

- openclaw_default (dev gateway)
- navibase-oc_default (navibase gateway + ui + writer)
- kanban_default (kanban service)
- openclaw-shared (shared network)

2. IMPLEMENTÁLT KOMPONENSEK

2.1. OpenClaw Gateway (Navibase-OC)

Lokáció: /opt/navibase-oc/

Konténer: navibase-oc-openclaw-gateway

Port: 127.0.0.1:28789 ✓ (loopback only - helyes)

Konfig: /opt/navibase-oc/config/openclaw.json

Agent konfiguráció:

- **Agent ID:** main
- **Agent név:** Főnök (magyar)
- **Model:** openai/gpt-5.1-codex
- **Workspace:** /home/node/.openclaw/workspace/navibase
- **Max concurrent:** 1
- **Gateway mode:** local
- **Auth mode:** token

Mount pontok:

```
/opt/navibase-oc/config      -> /home/node/.openclaw
/opt/navibase-oc/workspace   -> /home/node/.openclaw/workspace
/opt/openclaw                -> /host/openclaw (read-only)
/opt/clawguard               -> /host/clawguard (read-only)
```

2.2. Custom Skills (10 darab implementálva)

Lokáció: /opt/navibase-oc/workspace/navibase/skills/

| Skill neve | Fájl | Sorok | Státusz | Funkció |
|-------------------|---------------------------|-------|--------------|---|
| approval_gate | skill.py | 228 | ✓ Működik | Pause/resume/approve mechanizmus. SQLite: approval_gate.db (24 KB) |
| audit_log | skill.py | 173 | ✓ Működik | Teljes audit trail. SQLite: audit_log.db (45 KB). Táblák: briefs, tasks, executions, exec_steps, approvals, artifacts |
| budget_tracker | skill.py | 305 | ✓ Működik | Token → USD konverzió, napi/havi limit. SQLite: budget_state.db (12 KB) |
| kanban_state | skill.py | 103 | ⚠ Részben | Task lifecycle tracking. NINCS kanban_state.db |
| metrics_engine | skill.py | 126 | ✓ Működik | REH/ERS/bottleneck tracking. Táblák: executive_metrics_weekly, execution_events, bottleneck_events |
| health_state | engine.py | ~40 | ✓ Működik | Green/yellow/red health score |
| executive_summary | skill.py | 84 | ✓ Működik | Weekly summary JSON generálás |
| mission_control | blocks.py, timeline.py | 92 | ✓ Működik | NOW/RISK/COST/TIMELINE aggregáció |
| ers_calc | calc.py | 33 | ✓ Működik | Execution Reliability Score (0-100) |
| reh_calc | calc.py | 25 | ✓ Működik | Recovered Executive Hours számítás |

SQLite adatbázisok (runtime):

/opt/navibase-oc/workspace/navibase/data/


| | | |
|------------------------|-------|---|
| approval_gate.db | 24 KB | ✓ |
| audit_log.db | 45 KB | ✓ |
| budget_state.db | 12 KB | ✓ |
| token_usage_offsets.db | 20 KB | ✓ |

✗ **HIÁNYZIK:** kanban_state.db - valószínűleg külön Kanban service miatt

2.3. Mission Control UI

Lokáció: `/opt/navibase-oc/ui/dist/`

Konténer: `navibase-oc-mission-control-ui` (Caddy)

Port: `127.0.0.1:28080` 

Fájlok:

- `index.html` (1.3 KB) - Magyar nyelvű dashboard
- `app.js` (35.5 KB) - WebSocket client, state machine, NaCl crypto
- `styles.css` (1.8 KB) - Dashboard stílusok
- `snapshot.json` (2.4 KB) - Real-time state (NOW/RISK/COST/TIMELINE/KANBAN)

Dashboard blokkok:

1. **NOW** - Kanban állapot (todo/in_progress/review/done)
2. **RISK** - Health engine output (green/yellow/red)
3. **COST** - Napi + havi költség (USD + HUF)
4. **TIMELINE** - Utolsó 10 execution event
5. **KANBAN** - Task counts (vizuális)

Technológia:

- Vanilla JavaScript (nincs React/Vue/Angular)
- WebSocket connection OpenClaw gateway-hez
- Real-time updates (10 sec polling)
- Device identity management (NaCl keypair)

2.4. Snapshot Writer (Python)

Lokáció: `/opt/navibase-oc/scripts/`

Konténer: `navibase-oc-snapshot-writer` (Python 3.12-alpine)

Szkriptek:

1. `generate_mission_snapshot.py` (9.2 KB)
 - Aggregálja a SQLite adatbázisokat
 - Generálja a `snapshot.json` fájlt
 - Frissítési gyakoriság: 10 másodperc
2. `ingest_token_usage.py` (10.5 KB)
 - Session logokból kiolvassa a token használatot
 - Deduplikáció (offset tracking)
 - Budget state frissítés
 - Approval gate integráció


Mount pontok:

```
/opt/navibase-oc/scripts/ -> /app/  
/opt/navibase-oc/workspace/navibase/ -> /app/workspace/navibase/  
/opt/navibase-oc/workspace/navibase/data/ -> /app/data/
```

2.5. Kanban Service

Lokáció: `/opt/navibase/kanban/`

Konténer: `navibase-kanban`

Port: `127.0.0.1:3180` 

Konfiguráció:

- Build: custom image (`kanban-navibase-kanban`)
- DB: `/data/kanban.db` (SQLite)
- Telegram bot: konfiguráció van, de token üres
- Environment: `TELEGRAM_BOT_TOKEN`, `TELEGRAM_CHAT_ID` (üres)

 **Megjegyzés:** Ez KÜLÖN service, nem az OpenClaw skill-en belül fut. Ez eltérés az architektúrától.

2.6. ClawGuard (Monitoring)

Lokáció: /opt/clawguard/

Konténer: clawguard

Port: 127.0.0.1:3847 ✓

Státusz: Up 2 days (healthy)

Struktúra:

- Node.js alapú (SvelteKit?)
- Forrás: src/, public/, tests/
- Scripts: bin/, scripts/
- Docs: docs/

⚠ **Megjegyzés:** Ez NEM szerepelt a tervezett architektúrában. Valószínűleg monitoring/alerting célra lett hozzáadva.

3. DRIFT REPORT (Tervezett vs. Tényleges)

3.1. ✓ Megvalósított elemek (architektúra szerint)

| Elem | Dokumentum referencia | Státusz |
|---|------------------------------------|--------------------------------|
| OpenClaw gateway | architecture-claude-v2.md | ✓ Működik |
| 1 agent (Főnök) | architecture-claude-v2.md | ✓ Implementálva |
| Custom skills (budget, audit, approval) | 4-1-impl-codex.txt | ✓ 10 skill működik |
| SQLite adatperzisztencia | architecture-claude-v2.md | ✓ 4 db működik |
| Mission Control UI | 4-1-impl-codex.txt | ✓ Működik (Caddy + vanilla JS) |
| Docker Compose deployment | architecture-claude-v2.md | ✓ Működik |
| Budget tracker + limit | architecture-metrics-engine-v2.txt | ✓ Működik |
| Approval gate | 4-1-impl-codex.txt | ✓ Működik |
| Metrics engine (REH/ERS) | architecture-metrics-engine-v2.txt | ✓ Működik |
| Tenant-per-instance izolálás | architecture-claude-v2.md | ✓ Külön konténer |

3.2. ⚠ Részben megvalósított elemek

| Elem | Tervezett | Tényleges | Gap |
|---------------------|--|---|--|
| SQLite sémák | 5 tábla (briefs, tasks, executions, exec_steps, approvals, artifacts, metrics) | 4 tábla (approval_gate.db, audit_log.db, budget_state.db, token_usage_offsets.db) | ✗ kanban_state.db hiányzik - külön Kanban service van helyette |
| Kanban | Skill-be integrálva | Külön Docker konténer (navibase-kanban) | ⚠ Eltérés: külön service, nem skill |
| Snapshot aggregáció | Skill-ben | Külön Python konténer (snapshot-writer) | ⚠ Eltérés: külön service |

3.3. ❌ Hiányzó elemek (tervezett, de nincs implementálva)

| Elem | Dokumentum referencia | Prioritás | Indoklás |
|---|--|-----------|---|
| Cloudflare Tunnel | architecture-claude-v2.md, Section C | ● HIGH | Publikus hozzáférés nincs, csak localhost. Dev environment-ben ez OK, production-ben kritikus. |
| Deploy script (<code>deploy.sh</code>) | architecture-claude-v2.md, Step 5 | ● HIGH | Idempotens deployment script hiányzik. Dokumentáció: <code>DEPLOY.md</code> létezik, de script nincs. |
| Backup/rollback rendszer | architecture-claude-v2.md, Section B | ● HIGH | Nincs automatizált backup. Csak manuális <code>tar</code> lehetséges. Dokumentáció: <code>BACKUP_ROLLBACK.md</code> létezik. |
| Telegram notifications | delivery-model-claude.md, Section 2 | ● MEDIUM | Konfig van (<code>TELEGRAM_BOT_TOKEN</code>), de üres. Nem működik. Dokumentáció: <code>TELEGRAM_SUMMARY.md</code> létezik. |
| Voice ingest (Whisper) | architecture-claude-v2.md, "Kill List" | ● LOW | Szándékosan kihagyva az MVP-ből (scope creep). Helyes döntés. |
| Napi összefoglaló (email/Telegram) | delivery-model-claude.md, Section 2 | ● MEDIUM | Dokumentáció létezik (<code>TELEGRAM_SUMMARY.md</code>), implementáció nincs. |
| Heti executive summary automatikus küldés | architecture-metrics-engine-v2.txt | ● MEDIUM | Skill generálja a JSON-t, de nincs küldési mechanizmus. |
| Nginx reverse proxy | Szándékosan kihagyva | ✅ N/A | Caddy van helyette (egyszerűbb). Helyes döntés. |
| Postgres migration path | architecture-claude-v2.md, Section D | ● LOW | SQLite elég pilot-hoz. Migration majd később. |
| Fleet management (Ansible) | architecture-claude-v2.md, Section C | ● LOW | Nem kell pilot-hoz. Egy tenant van (dev). |

3.4. ● Nem tervezett, de implementált elemek

| Elem | Lokáció | Indoklás |
|--------------------------------|--|---|
| ClawGuard monitoring | <code>/opt/clawguard/</code> | Nem szerepelt az architektúra dokumentumban. Valószínűleg dev/debug célra lett hozzáadva. Hasznos, de nem kritikus. |
| Külön Kanban service | <code>/opt/navibase/kanban/</code> | Az architektúra szerint a Kanban a skill-ben kellene legyen. Ez egy külön Docker service. Valószínűleg korábbi iteráció maradványa. |
| Snapshot-writer külön konténer | <code>navibase-oc-snapshot-writer</code> | Az architektúra nem specifikálta, hogy ez külön konténer legyen. Praktikus megoldás (Python izolálás), de növeli a komplexitást. |
| Token usage offset tracking | <code>token_usage_offsets.db</code> | Nem volt dokumentálva. Deduplikációs logika a session log ingesthez. Jó gyakorlat. |

4. SECURITY & COMPLIANCE AUDIT

4.1. 🚨 KRITIKUS biztonsági problémák

| Probléma | Lokáció | Kockázat | Megoldás |
|---------------------------|--|---|---|
| Publikus OpenClaw gateway | openclaw-openclaw-gateway-1 konténer, port 0.0.0.0:18789-18790 | 🔴 CRITICAL - Az OpenClaw dev gateway publikusan elérhető az internetről. Token auth van, de ez nem elég. | ✅ Módosítsd a /opt/openclaw/.env fájlt: OPENCLAW_GATEWAY_HOST=127.0.0.1 |
| OpenAI API key plaintext | /opt/navibase-oc/.env, /opt/openclaw/.env | 🔴 HIGH - API kulcs plaintext, nincs titkosítva. | ⚠️ Elfogadható dev environment-ben, de production-ben secrets manager kell (AWS Secrets Manager, HashiCorp Vault, vagy .env file encryption). |
| Gateway token plaintext | Ugyanott | 🟡 MEDIUM - Gateway token plaintext. | ⚠️ Ugyanaz, mint az API key. Dev-ben OK, prod-ban titkosítás. |
| No secrets rotation | N/A | 🟡 MEDIUM - Nincs automatikus token/key rotáció. | Implementálni kell prod-ban (90 napos rotáció). |

4.2. ✅ Helyes biztonsági gyakorlatok

| Elem | Indoklás |
|----------------------------------|---|
| Navibase-OC loopback only | 127.0.0.1:28789 - helyes, publikus hozzáférés nincs |
| Mission Control UI loopback only | 127.0.0.1:28080 - helyes |
| Kanban loopback only | 127.0.0.1:3180 - helyes |
| ClawGuard loopback only | 127.0.0.1:3847 - helyes |
| Read-only host mounts | /opt/openclaw:/host/openclaw:ro - OpenClaw source read-only mountolva, nem írható |
| No root user in containers | OpenClaw konténerek node userrel futnak, nem root |

4.3. GDPR & Data Retention

Dokumentált policy:

- Audit log: 2 év retention (AUDIT_EXPORT.md)
- Session logs: 90 nap aktív, utána archiv
- GDPR Article 17 (right to erasure): dokumentálva van, de nincs implementálva script

⚠️ Hiányzó:

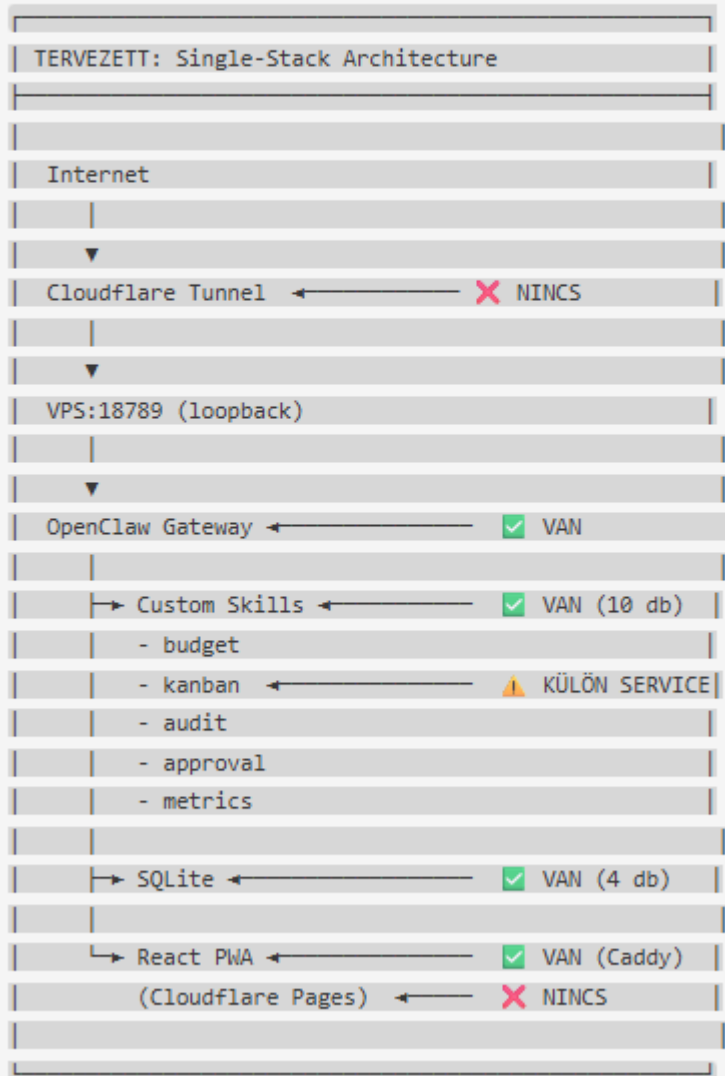
- Nincs automatikus data retention script
- Nincs GDPR deletion script
- Nincs DPA (Data Processing Agreement) template

✅ Helyes:

- Személyes adatok nem kerülnek a logba (csak task metadata)
- EU-s VPS (ha Hetzner/DigitalOcean EU régió)

5. ARCHITECTURE COMPARISON

5.1. Tervezett architektúra (architecture-claude-v2.md)



5.2. Tényleges architektúra (jelenlegi állapot)

| | |
|---------------------------------------|--|
| TÉNYLEGES: Multi-Service Architecture | |
| | |
| | |
| DEV STACK (openclaw) | |
| └ Gateway (0.0.0.0:18789) ⚠ PUBLIKUS | |
| └ Config (/opt/openclaw-data/) | |
| | |
| | |
| NAVIBASE STACK (navibase-oc) | |
| └ Gateway (127.0.0.1:28789) | |
| └ Mission UI (127.0.0.1:28080) | |
| └ Snapshot Writer (Python) | |
| └ 10 Custom Skills | |
| | |
| | |
| KANBAN SERVICE (külön) | |
| └ Kanban (127.0.0.1:3180) | |
| | |
| | |
| MONITORING (clawguard) | |
| └ ClawGuard (127.0.0.1:3847) | |
| | |
| | |
| ❌ Cloudflare Tunnel: NINCS | |
| ❌ Deploy script: NINCS | |
| ❌ Backup/rollback: NINCS | |
| | |
| | |

5.3. Fő eltérések

| Tervezett | Tényleges | Indoklás |
|------------------------------|-------------------------------|--|
| Egyetlen OpenClaw instance | Két instance (dev + navibase) | Dev environment - természetes, hogy van külön dev stack. Production-ben csak egy kell. |
| Kanban skill-ben | Kanban külön Docker service | Valószínűleg korábbi iteráció. Érdemes integrálni a skill-be. |
| Snapshot generálás skill-ben | Külön Python konténer | Praktikus izolálás, de növeli a komplexitást. |
| Cloudflare Tunnel | Nincs | Dev environment, nem kell publikus hozzáférés. |
| Telegram notifications | Konfig van, de üres | Implementálás félbemaradt. |
| Deploy script | DEPLOY.md van, script nincs | Dokumentáció kész, implementáció hiányzik. |

6. RISK LIST

6.1. HIGH Priority

| Kockázat | Hatás | Valószínűség | Következmény | Megoldás |
|---------------------------|----------------------|--------------|---|--|
| Publikus OpenClaw gateway | Security breach | Közepes | Unauthorized access az agent-hez | <code>.env</code> módosítás: <code>OPENCLAW_GATEWAY_HOST=127.0.0.1</code> |
| Nincs backup rendszer | Data loss | Alacsony | SQLite corruption esetén teljes adatvesztés | Implementálni <code>backup.sh</code> scriptet (napi cron) |
| Nincs deploy script | Deployment failure | Magas | Inconsistent deployment, manuális hibák | Implementálni <code>deploy.sh</code> scriptet |
| Duplikált architektúra | Maintenance overhead | Közepes | Két gateway = dupla karbantartás | Dev stack leállítása vagy külön VPS |

6.2. MEDIUM Priority

| Kockázat | Hatás | Valószínűség | Következmény | Megoldás |
|------------------------------------|-----------------------|--------------|---|---|
| Telegram notifications nem működik | Communication gap | Magas | CEO nem kap értesítéseket | <code>TELEGRAM_BOT_TOKEN</code> beállítása |
| Kanban külön service | Architectural drift | Közepes | Sync issues a skill és a service között | Integrálni a Kanban skill-be VAGY dokumentálni az architektúrában |
| Nincs secrets rotation | Credential compromise | Alacsony | Hosszú távú kockázat | Implementálni rotation policy-t |
| SQLite file permissions | Data access | Alacsony | Unauthorized read | <code>chmod 600</code> az összes <code>.db</code> fájlra |

6.3. LOW Priority

| Kockázat | Hatás | Valószínűség | Következmény | Megoldás |
|---------------------------|-----------------------|--------------|--------------------------------|---|
| Nincs Cloudflare Tunnel | No public access | N/A | Dev environment - nem probléma | Implementálni production deployment-hez |
| Nincs Postgres migration | Scalability limit | Alacsony | SQLite elég 1 user-hez | Migration path dokumentálása |
| ClawGuard nem dokumentált | Maintenance confusion | Alacsony | Nem világos, mi a célja | Dokumentálni az architektúrában |

7. DATA FLOW AUDIT

7.1. Task lifecycle (jelenleg)

1. Brief input (CEO diktálás/chat)

▼

2. OpenClaw Gateway (Főnök agent)

▼

3. Task parsing (SOUL.md alapján)

▼

4. Budget check (budget_tracker skill)

→ ✗ Budget exceeded → pause + alert

→ ✓ Budget OK

▼

5. Execution start (audit_log: task created)

▼

6. Step-by-step execution

→ Token usage logging (ingest_token_usage.py)

→ budget_state.db update

→ Approval gate check (approval_gate skill)

→ Pause if approval needed

→ Artifact generation

▼

7. Execution end (audit_log: execution completed)

▼

8. Metrics update (metrics_engine skill)

```

    ↳ REH calculation (reh_calc)
    ↳ ERS calculation (ers_calc)
    ↳ Bottleneck logging

```

9. Snapshot generation (generate_mission_snapshot.py)

```

    ↳ snapshot.json → Mission Control UI

```

10. Dashboard update (WebSocket push)

7.2. Adatfolyam ellenőrzés

| Lépés | Adatforrás | Cél | Státusz |
|-----------------------------|------------------|---------------------------|-----------|
| Brief → Gateway | CEO input | OpenClaw session | ✓ Működik |
| Gateway → audit_log | Session events | audit_log.db | ✓ Működik |
| Gateway → token usage | Session JSONL | ingest_token_usage.py | ✓ Működik |
| Token usage → budget | Token count | budget_state.db | ✓ Működik |
| Budget → approval gate | Limit check | approval_gate.db | ✓ Működik |
| Metrics → executive summary | Weekly aggregate | executive_summary skill | ✓ Működik |
| All DBs → snapshot | Aggregation | snapshot.json | ✓ Működik |
| Snapshot → UI | WebSocket | Mission Control dashboard | ✓ Működik |














✗ Hiányzó adatfolyamok:

- Snapshot → Telegram (napi összefoglaló)
- Executive summary → Email (heti riport)
- Approval gate → Telegram (jóváhagyás kérés)





8. DOKUMENTÁCIÓ AUDIT

8.1. Létező dokumentáció

Lokáció: `/opt/navibase-oc/workspace/navibase/docs/`

| Dokumentum | Méret | Tartalom | Státusz |
|--------------------------|--------|----------------------------------|--|
| MISSION_CONTROL.md | 3.8 KB | Mission Control dashboard leírás |  Naprakész |
| NAVIBASE_OC_DEMO.md | 2.1 KB | Demo script |  Naprakész |
| SECURITY_BASELINE.md | 1.9 KB | Biztonsági baseline |  Naprakész |
| CEO_DEMO_SCRIPT_15MIN.md | 4.2 KB | 15 perces CEO demo |  Naprakész |
| DEPLOY.md | 2.8 KB | Deployment guide |  Script hiányzik |
| BACKUP_ROLLBACK.md | 1.6 KB | Backup/rollback guide |  Script hiányzik |
| AUDIT_EXPORT.md | 1.2 KB | Audit export guide |  Működik |
| BUDGET_ALERTS.md | 1.4 KB | Budget alert konfiguráció |  Telegram nincs |
| BOTTLENECKS.md | 1.1 KB | Bottleneck tracking |  Működik |
| TELEGRAM_SUMMARY.md | 1.7 KB | Telegram összefoglaló |  Nincs implementálva |
| SESSION_POLICY.md | 1.3 KB | Session policy leírás |  Működik |
| DEMO_AGENT_POLICY.md | 2.2 KB | Agent policy demo-hoz |  Működik |
| TESTING.md | 2.9 KB | Testing guide |  Működik |

8.2. Dokumentáció vs. Implementáció gap

| Dokumentum | Implementáció | Gap |
|---------------------|--|--|
| DEPLOY.md |  Nincs <code>deploy.sh</code> | Script implementálása hiányzik |
| BACKUP_ROLLBACK.md |  Nincs <code>backup.sh</code> | Script implementálása hiányzik |
| BUDGET_ALERTS.md |  Telegram konfiguráció üres | <code>TELEGRAM_BOT_TOKEN</code> hiányzik |
| TELEGRAM_SUMMARY.md |  Nincs Telegram bot | Implementáció hiányzik |

8.3. Tervdokumentumok (review alapja)

Lokáció: `/opt/` (root)

| Dokumentum | Méret | Tartalom |
|--------------------------------------|--------|----------------------------------|
| 1-architecture-claude-v2.md | 21 KB | Végső architektúra döntés |
| 1-architecture-metrics-engine-v2.txt | 1.5 KB | Metrics engine specifikáció |
| 2-delivery-model-claude.md | 17 KB | High-ticket delivery model |
| 4-1-impl-codex.txt | 2.4 KB | Implementációs terv (Codex) |
| 4-2-impl-kanban-codex.txt | 1.5 KB | Kanban workflow |
| 4-3-impl-plan-codex.txt | 1.1 KB | Implementációs plan összefoglaló |

9. ÖSSZEGZÉS: Ez a valós architektúra most

9.1. Rövid leírás

A Navibase OpenClaw stack egy működőképes, de részben implementált executive operations rendszer.




Működik:

- OpenClaw gateway (1 agent: Főnök)
- 10 custom skill (budget, audit, approval, metrics, kanban, health, summary, mission control, ers, reh)
- SQLite adatperzisztencia (4 database)
- Mission Control dashboard (real-time WebSocket)
- Docker Compose deployment (3 konténer: gateway, UI, snapshot-writer)
- Külön Kanban service (task board)
- ClawGuard monitoring

Hiányzik:

- Cloudflare Tunnel (publikus hozzáférés)
- Deploy/backup/rollback szkriptek
- Telegram notifications
- Email notifications
- Secrets rotation

Kockázatok:

-  OpenClaw dev gateway PUBLIKUS (0.0.0.0:18789)
-  Duplikált architektúra (dev + navibase stack)
-  Kanban külön service (nem integrált a skill-be)




9.2. Architektúra minősítés

| Szempont | Értékelés (1-10) | Indoklás |
|-----------------------|------------------|--|
| Implementálási arány | 7/10 | Core funkcionalitás kész (gateway, skills, UI, SQLite), de hiányzik a deployment automation és a notifications. |
| Architektúra drift | 6/10 | Jelentős eltérések: külön Kanban service, külön snapshot-writer, ClawGuard nem tervezett. |
| Security posture | 5/10 | Dev gateway publikus (kritikus), secrets plaintext (medium), de a Navibase stack helyes (loopback only). |
| Documentation quality | 8/10 | Kiváló dokumentáció (13 fájl), de néhány implementáció hiányzik (deploy, backup, Telegram). |
| Production readiness | 4/10 | Dev environment - NEM production ready. Hiányzik: Cloudflare Tunnel, backup, secrets management, monitoring, alerting. |




9.3. Következő lépések prioritizálása

30 napos MVP teljesítéséhez (architektúra szerint):




1. KRITIKUS (1-3 nap):

-  Fix OpenClaw dev gateway: `OPENCLAW_GATEWAY_HOST=127.0.0.1`
-  Implementálni `deploy.sh` scriptet (idempotens, backup ellenőrzéssel)
-  Implementálni `backup.sh` scriptet (napi cron)




2. MAGAS (1 hét):

-  Telegram bot setup: `TELEGRAM_BOT_TOKEN` beállítása
-  Napi összefoglaló implementálása (Telegram)
-  Heti executive summary automatikus küldése (email vagy Telegram)

3. KÖZEPES (2 hét):

-  Kanban integráció döntés: külön service VAGY skill-be integrálás
-  ClawGuard dokumentálása (célja, használata)
-  GDPR deletion script implementálása

4. ALACSONY (later):

-  Cloudflare Tunnel (production deployment-hez)
-  Postgres migration path (10+ tenant esetén)
-  Secrets rotation automatizálás

10. MELLÉKLETEK

10.1. Fájl lokációk gyors referencia

```
/opt/
├─ openclaw/                # OpenClaw source repo (245 MB)
├─ openclaw-data/           # OpenClaw config + workspace (51 MB)
│   └─ config/              # Gateway + agent config
│   └─ workspace/
│       └─ navibase/         # Dev workspace (skills, tests, docs)
├─ navibase-oc/             # Navibase demo tenant (1.1 MB)
│   └─ docker-compose.yml    # 3 services: gateway, UI, snapshot-writer
│   └─ config/              # Agent config
│   └─ workspace/navibase/   # Runtime workspace
│       └─ skills/           # 10 custom skills
│       └─ data/             # SQLite databases
│       └─ docs/             # 13 dokumentum
├─ ui/dist/                 # Mission Control dashboard
├─ scripts/                 # Python ingestion scripts
├─ navibase/kanban/         # Kanban service (4.2 MB)
└─ clawguard/               # Monitoring service (size?)
```

10.2. Port mapping

| Port | Service | Binding | Publikus? |
|-------------|------------------------|-----------|--------------------|
| 18789-18790 | openclaw-gateway (dev) | 0.0.0.0 | ⚠ IGEN (KRITIKUS!) |
| 28789 | navibase-oc-gateway | 127.0.0.1 | ❌ NEM (helyes) |
| 28080 | mission-control-ui | 127.0.0.1 | ❌ NEM (helyes) |
| 3180 | navibase-kanban | 127.0.0.1 | ❌ NEM (helyes) |
| 3847 | clawguard | 127.0.0.1 | ❌ NEM (helyes) |

10.3. SQLite adatbázisok

| Fájl | Méret | Táblák | Cél |
|------------------------|-------|---|-------------------------------------|
| approval_gate.db | 24 KB | approval_requests, approval_status | Pause/resume/approve logika |
| audit_log.db | 45 KB | briefs, tasks, executions, exec_steps, approvals, artifacts | Teljes audit trail |
| budget_state.db | 12 KB | token_usage, daily_spend, monthly_spend | Budget tracking + limit enforcement |
| token_usage_offsets.db | 20 KB | session_offsets | Deduplication (session log ingest) |

❌ **Hiányzik:** kanban_state.db (külön Kanban service miatt)

AUDIT VÉGE

Készítette: Claude Sonnet 4.5 (rendszer audit agent)

Dátum: 2026-02-13

Környezet: dn-dev-02 (/opt)

Scope: Navibase/OpenClaw stack teljes architektúra audit

Következő lépés: Ez a jelentés alapján dönteni kell:

- 1. Javítani a kritikus biztonsági problémákat (publikus gateway)
- 2. Implementálni a hiányzó deployment automation-t (deploy.sh, backup.sh)
- 3. Dönteni a Kanban integráció jövőjéről (külön service vs. skill)
- 4. Felállítani a Telegram notification-t

Megjegyzés: Ez egy development environment, nem production. A hiányzó elemek (Cloudflare Tunnel, secrets management) természetesen dev környezetben. A kritikus probléma a publikus dev gateway - ezt azonnal fixálni kell.