DNS & Domain Inventory Verification Protocol

DNS & Domain Inventory Verification Protocol

Rule ID: DNS-VERIFY-001
Effective Date: 2026-04-20
Owner: FlowForge (DevOps)
Applies To: All agents adding domains to hosting platforms or inventory docs

---

Rule Statement

Every domain added to hosting platforms or ALAI inventory MUST pass DNS + RDAP registry verification BEFORE deployment or documentation.

This rule prevents typos, phantom domains, and inventory errors from propagating through systems.

When This Rule Applies

BEFORE any of these actions:

1. Adding domain to hosting platform (Vercel, Cloudflare Pages, GCP, Azure)
2. Updating alai-hosting-inventory.md with new domain
3. Creating DNS records (A, CNAME, NS)
4. Documenting client domains in BookStack
5. Writing domain into specs, blueprints, or task descriptions

Triggers:

- Client provides new domain for hosting

- Migrating domain between platforms
- Registering new domain for ALAI product
- Auditing existing inventory

Verification Steps

1. DNS Resolution Check

Command:

```
dig +short {DOMAIN} A
```

Expected output:

- If domain is NEW: empty output or registrar parking IP
- If domain is EXISTING: should return hosting provider IPs

2. RDAP Registry Check (PRIMARY VALIDATION)

Purpose: Verify domain is actually registered in TLD registry (catches typos)

Command:

```
curl -sS "https://rdap.nic.{TLD}/domain/{DOMAIN}" | jq -r '.handle // .ldhName // "NOT_FOUND"'
```

TLD-specific RDAP servers:

TLD	RDAP Base URL
.no	https://rdap.norid.no/domain/
.com	https://rdap.verisign.com/com/v1/domain/
.io	https://rdap.nic.io/domain/
.pro	https://rdap.nic.pro/domain/
.ba	(no public RDAP, use WHOIS)
.rs	(no public RDAP, use WHOIS)

Expected output:

- Valid domain: Returns handle/ldhName (e.g., DONUTS_14F30DC66CE34C0A89C4A31B5CD73FE1-PRO)
- Invalid/typo: HTTP 404 or "NOT_FOUND"

3. WHOIS Fallback (for TLDs without RDAP)

Command:

```
whois {DOMAIN} | grep -i "domain name\|status\|registrar"
```

4. Registrar Identification

Command (via RDAP):

```
curl -sS "https://rdap.nic.{TLD}/domain/{DOMAIN}" | jq -r '.entities[] | select(.roles[] == "registrar") | .vcardArray[1][] | select(.[0] == "fn") | .[3]'
```

Purpose: Replace generic "Third Party" with actual registrar name

5. Expiry Date Check

Command (via RDAP):

```
curl -sS "https://rdap.nic.{TLD}/domain/{DOMAIN}" | jq -r '.events[] | select(.eventAction == "expiration") | .eventDate'
```

Failure Actions

If domain fails RDAP check (404 error):

DO NOT:

- Add domain to hosting platform
- Write domain into inventory docs
- Configure DNS records
- Deploy site to that domain

INSTEAD:

1. **Verify spelling with client/team**
2. **Check if domain is registered**
3. **Flag as TYPO_OR_MISSING status**
4. **Update requester**

Inventory Standards

Required fields for every domain entry:

Domain	Registrar	NS Provider	Hosting	Repo	Stack	Expiry	Status
example.com	Namecheap	Cloudflare	CF Pages	~/path	Next.js	2027-01-15	□ LIVE

Field validation:

- **Domain:** Must pass RDAP check
- **Registrar:** NEVER "(Third Party)" — get real name from RDAP
- **Expiry:** REQUIRED (YYYY-MM-DD format)
- **Status:** □ LIVE | ⚠ STALE | □ DOWN | □□ MAINTENANCE

Incident: kenyhot.pro Typo (2026-04-20)

What happened:

- Domain registered as kenyhot.pro at Namecheap (correct spelling)
- Entered into Vercel as knyhot.pro (missing "e")
- Phantom domain knyhot.pro does NOT exist in .pro registry
- Typo propagated to inventory docs, blueprints, 2 Vercel projects
- Caught 29 days later during hosting audit

Why this rule prevents it:

- RDAP check for knyhot.pro returns 404 → immediate red flag
- Would have forced spelling verification before Vercel setup
- Automated inventory sync would reject domain without valid RDAP response

Prevention checklist:

- □ RDAP check before Vercel domain add
- □ Registrar lookup (never use "Third Party")
- □ Expiry date recorded
- □ Inventory changelog entry
- □ Evidence folder created

Exceptions

This rule does NOT apply to:

1. **Internal-only domains** (localhost, *.local, *.internal)
2. **Development subdomains** on verified parent domain
3. **IP-based access** (e.g., Azure VM via IP)

Partial verification for:

- **.ba / .rs domains** — Use WHOIS only (no public RDAP servers)
- **Recently registered domains** — RDAP may take 24-48h to propagate

---

Compliance

Enforcement:

- FlowForge will reject any hosting setup without verification evidence
- CodeCraft/Vizu: do NOT update site content referencing unverified domains
- John: gate-check all domain additions in MC tasks

Audit frequency:

- Quarterly inventory verification (re-run RDAP on all domains)
- Flag expiring domains (< 60 days)
- Remove phantom/typo entries

References:

- IANA RDAP Bootstrap: https://data.iana.org/rdap/
- RFC 7483: https://datatracker.ietf.org/doc/html/rfc7483
- Incident post-mortem: /Users/makinja/system/evidence/kenyhot-vercel-cleanup/

Related Rules:

- INFRA-001: Hosting platform standards
- DOC-002: Inventory accuracy requirements

Created by: ALAI, 2026
Last synced: 2026-04-20
Source: /Users/makinja/system/rules/dns-inventory-verification.md

---

Revision #2
Created 2026-04-20 19:10:19 UTC by John
Updated 2026-05-31 20:06:20 UTC by John