

DNS & Domain Architecture

sbsdash.com zone, three-subdomain tenant model, record inventory, DNSSEC

- [Chapter 4 — DNS & Domain Architecture](#)

Chapter 4 — DNS & Domain Architecture

4.1 Domain and Registrar

`sbsdash.com` is the sole Platform domain. Registrar-level state is a security control surface in its own right (DNS-01):

- **Ownership (target)** — the domain is registered to SBS (org-level contact, SBS-controlled email alias — same survivability rationale as the DigitalOcean account, §2.1). The Build Register carries the domain transfer item ("Transfer SBSDASH.COM") until registrar ownership sits with SBS; the current registration under the interim account is a tracked transitional state.
- **Registrar lock** — `clientTransferProhibited` enabled; transfer-out requires an authenticated unlock action. Domain-transfer attempts are a high-severity alert.
- **Registrar MFA** — phishing-resistant MFA on the registrar account. IAM-03 applies to every control plane, registrar included: registrar compromise is functionally equivalent to full platform compromise, since it permits nameserver redelegation.
- **Renewal** — auto-renew enabled, multi-year registration, expiry monitored (an expired domain is simultaneously an availability failure and a takeover opportunity).

4.2 Authoritative DNS

As built (2026-07-18): the zone is hosted on **GoDaddy nameservers**. GoDaddy does not provide DNSSEC signing for externally manageable zones in this configuration, records are console-managed rather than IaC-managed, and no API-driven change control is in place. This state satisfies neither DNS-01 (DNSSEC) nor the IaC management rule (Chapter 10) and is a tracked nonconformance (Build Register item 9).

Target: the authoritative zone is hosted at a DNSSEC-capable, API-managed provider. Approved options, in preference order:

1. **Cloudflare DNS** (free tier sufficient) — one-click DNSSEC signing, DS handoff to the registrar, full API for IaC management, native CAA/CT tooling.
2. **deSEC** — DNSSEC-by-default, API-managed, nonprofit.
3. Registrar-hosted DNS **only if** the registrar signs zones and exposes a management API.

Zone cutover sequence (Nelson Santos, execution owner): replicate the current record set at the new provider → verify resolution parity against §4.3 → lower TTLs to 300 → update NS delegation at the registrar → confirm propagation → enable DNSSEC and publish DS (§4.5) → raise TTLs. The zone

is thereafter managed as code (Chapter 10): records are defined in the IaC repository and applied via provider API; console edits are drift and reverted.

4.3 Record Inventory

As built (2026-07-18):

Record	Type	Value (actual)	State
sbsdash.com	A	138.197.222.154 (Dev-Gitlab-server) ⚠	Nonconformant — apex resolves to an uninventoried dev host, not prod (§2.2.2, Build Register item 16)
monitor.sbsdash.com	A	162.243.28.132 (monitor-servers)	Live and verified — TLS valid, Grafana responding (changelog 2026-07-17)
wiki.sbsdash.com	A	167.172.135.88 (sbs-wiki, NYC1)	Live; IP changes at NYC2 rebuild
admin.sbsdash.com, clients.sbsdash.com, www	—	Not yet published	Pending prod proxy/TLS readiness (Chapter 5)

Target:

Record	Type	Value	TTL	Serves
sbsdash.com	A	107.170.72.145	300 (build) → 3600 (steady)	Primary tenant surface — repointed from 138.197.222.154 at cutover
www.sbsdash.com	CNAME	sbsdash.com	3600	Redirect to apex at proxy
admin.sbsdash.com	A	107.170.72.145	300 → 3600	Administrative console
clients.sbsdash.com	A	107.170.72.145	300 → 3600	Client-facing surface
monitor.sbsdash.com	A	162.243.28.132	3600	Grafana/Prometheus (IdP-gated)
wiki.sbsdash.com	A	NYC2 rebuild IP	300 until rebuild, then 3600	BookStack portal

Notes:

- Tenant surfaces share one A target; host-header routing at the reverse proxy (Chapter 5) separates them. No wildcard record exists — *.sbsdash.com is unresolvable by design (FE family: no surface enumeration; a wildcard would also pollute the CT-monitoring signal, §4.6).

- The apex repoint (138.197.222.154 → 107.170.72.145) is executed only after the prod proxy and TLS stack pass their Chapter 5 gates — repointing to an unready origin is an availability failure. Until then the current apex target remains inside the engagement security boundary (§2.2.2).
- Dev has **no** records in the public zone. The as-built apex record violates this rule today; it is cured by the repoint. Dev access is by IP against the admin allowlist.
- IPv6: AAAA records are added only when droplet IPv6 is enabled *and* firewall rulesets carry mirrored v6 rules — publishing AAAA without v6 firewall parity is a firewall bypass, so the two land together or not at all. (As built there are no v6 firewall rules anywhere; no AAAA records are published.)

4.4 Mail Posture (DNS-03)

`sbsdash.com` sends and receives no mail. Null-mail posture, published explicitly so the domain cannot be used as a spoofed sender:

Record	Type	Value
<code>sbsdash.com</code>	MX	<code>0 .</code> (null MX, RFC 7505)
<code>sbsdash.com</code>	TXT	<code>v=spf1 -all</code>
<code>_dmarc.sbsdash.com</code>	TXT	<code>v=DMARC1; p=reject; adkim=s; aspf=s; rua=mailto:<SBS security alias></code>

These records are publishable on GoDaddy **today** — they do not depend on the zone cutover and should not wait for it. DMARC aggregate reports route to an SBS security mailbox on an existing SBS mail domain (not `sbsdash.com`), making spoof attempts observable — a MON-02 anomaly input, not merely a static record.

One caution: the Grafana admin account and the changelog reference `admin@sbsdash.com` and a Yahoo mailbox as service identities. No mailbox exists or will exist on `sbsdash.com` under the null-mail posture; service accounts must use SBS-controlled aliases on SBS's mail domain. Folded into the credential remediation (Build Register item 15).

4.5 DNSSEC (DNS-01)

As built: unsigned — no signing path exists on the current GoDaddy hosting (§4.2). DNS-01 is unmet until zone cutover completes.

Target, unchanged in substance:

- Zone signed at the DNS provider (ECDSA P-256, algorithm 13 — compact signatures, universal resolver support).
- **DS record published at the registrar** — signing without registrar DS publication provides no validation path. End-to-end verification: `dig +dnssec sbsdash.com` returns the AD flag from a validating resolver, and DNSViz shows an unbroken chain. This verification is a named Build Register gate (item 10).

- Key rollovers are provider-automated (CDS/CDNSKEY where the registrar supports it); manual DS changes are change-controlled.
- Failure-mode note: DNSSEC misconfiguration causes hard resolution failure, not degraded security — DS/keyset changes execute inside the 300-TTL window and are verified before TTLs are raised.

4.6 Certificate and Registration Surveillance

- **CAA (DNS-02):** `sbsdash.com CAA 0 issue "letsencrypt.org"` plus `CAA 0 iodef "mailto:<SBS security alias>"`. Only Let's Encrypt may issue for the domain — consistent with the deployed ACME/certbot practice already live on `monitor.sbsdash.com` (Let's Encrypt via certbot, auto-renewal by systemd timer, per changelog 2026-07-17). Any other CA refusing on CAA is the control working. `issuewild` is intentionally absent (inherits `issue`; acceptable — no wildcard certificates are used). Publishable on GoDaddy today; does not wait for cutover.
- **CT monitoring (DNS-04):** subscription against Certificate Transparency logs for `sbsdash.com` (Cloudflare CT alerts or crt.sh RSS into the alert pipeline). Baseline note: certificates for `monitor.sbsdash.com` already appear in CT from the 2026-07-17 issuance — expected and legitimate. Any CT appearance **not** originating from the platform's ACME automation is a high-severity incident (CAA bypass or issuance compromise).
- **Typosquat monitoring (DNS-05):** dnstwist scheduled weekly from `monitor-servers` against a generated permutation set (homoglyphs, transpositions, TLD swaps); newly registered lookalikes feed MON-02 alerting. No defensive registrations by default; escalation case-by-case via Alexandra Del Rey (security-compliance routing).

4.7 Change Control and Verification

Until zone cutover, GoDaddy console changes are restricted to: the three mail records (§4.4), the CAA record (§4.6), and the apex repoint (§4.3) — each logged in `SERVER_CHANGELOG.md` with date and operator. After cutover, zone changes follow the IaC path (Chapter 10) with the same drift rules as firewalls.

Verification gates: NS delegation at registrar points to the DNSSEC-capable provider; DNSSEC chain validates (AD flag, DNSViz clean); null-MX/SPF/DMARC present; CAA present; apex and all subdomain records resolve per the §4.3 target table (apex → 107.170.72.145, not 138.197.222.154); no wildcard resolves; no Dev host referenced anywhere in the zone. Controls covered: DNS-01 through DNS-05.

Build Register deltas from this chapter: item 9 restated as GoDaddy→provider cutover with sequence; item 16 apex repoint gated on Chapter 5 readiness; **new item 23** — publish null-mail + CAA records on GoDaddy immediately (pre-cutover); item 15 extended to cover the `admin@sbsdash.com` / Yahoo service-identity cleanup. Chapter 5 (TLS & Edge Security) next — the monitor's live nginx/certbot stack gives it a verified as-built baseline to write against.