Appendices

Resource inventory, firewall rule table, acronym table, references (NIST SP 800-207, OWASP ASVS L2)

Chapter 18 — Appendices

Appendix A — Resource Inventory

A.1 DigitalOcean Account & Projects

Resource	Identifier	Notes
DO Account	SBS-owned (alias ownership pending, §2.1)	MFA/team-audit pending item 15/17 chain
Project: SBS The Dash Dev	`ac656e28-2196-410e-847c-bf3b60363710`	Default project
Project: SBS The Dash Prod	`c49c646f-f268-4b51-a00e-ad9fb5055569`	

A.2 Droplets (As Built)

Droplet	Project	Region / VPC	Size	Public IP	Private IP	OS	Role	DO Backups
`Dev-SBS-server`	Dev	NYC2 / default-nyc2	8 GB / 4 vCPU / 160 GB	162.243.252.138	10.100.0.2	Ubuntu 24.04	Dev server; Docker 29.1.3	□ (target: weekly)
`sbsdash-server-prod`	Prod	NYC2 / default-nyc2	8 GB / 4 vCPU / 160 GB	107.170.72.145	10.100.0.3	TBC	Prod app; tenant surfaces; Docker 29.1.3; bastion-only SSH	□ (target: daily)
`monitor-servers`	Prod	NYC2 / default-nyc2	4 GB / 2 vCPU / 120 GB	162.243.28.132	10.100.0.4	Ubuntu 26.04	Grafana 13.1.0 / Prometheus / nginx 1.28.3 / Loki (planned); bastion	□ (target: daily)
`sbs-wiki`	Prod	**NYC1 / default-nyc1** ⚠	2 GB / 1 vCPU / 60 GB	167.172.135.88	10.116.0.2	TBC	BookStack; NYC2 rebuild pending	□ (target: daily)
`Dev-Gitlab-server` ⚠	Unregistered	VPC 10.120.x	TBC	138.197.222.154	TBC	TBC	**Holds apex DNS**; disposition item 22	Pre-repoint backup: item 101

Droplet	Project	Region / VPC	Size	Public IP	Private IP	OS	Role	DO Backups
`prod-vault`	Prod	NYC2 / prod-vpc-nyc2	1 GB / 1 vCPU	—	—	—	**Planned** — Vault (§8.2), rebuild wave	Daily at creation

A.3 Network (Target vs. As Built)

Network	CIDR	State
`prod-vpc-nyc2`	10.10.0.0/20	Target — rebuild wave (item 18/59)
`dev-vpc-nyc2`	10.20.0.0/20	Target — rebuild wave
`default-nyc2`	10.100.0.0/20	As built — Dev+Prod shared ⚠, vacated at rebuild
`default-nyc1`	10.116.0.0/20	As built — wiki only, vacated at rebuild

A.4 DNS Zone (sbsdash.com — GoDaddy NS, cutover pending item 9)

Record	Target (as built)	Target (spec)
apex A	138.197.222.154 ⚠	107.170.72.145 (item 16, gated on Ch. 5)
www CNAME	—	sbsdash.com
admin A / clients A	—	107.170.72.145
monitor A	162.243.28.132 □ live+TLS	unchanged
wiki A	167.172.135.88	NYC2 rebuild IP
MX / SPF / DMARC / CAA	absent	null-mail + LE-only CAA (item 23 — publishable now)

A.5 Storage & Registry (Planned)

Resource	Location	Chapter
Spaces: `sbs-dash-artifacts`, `sbs-dash-audit`, `sbs-dash-backups`	NYC3 (+SFO3 replication)	§7.3, §13, §14
DO Volumes: data engines, Loki, audit writer, Vault Raft	NYC2	§7.6, §12.3, §13.3, §8.2
GHCR (SBS org)	—	§11.2
Repos: `sbs-dash-infra`, platform app repo	GitHub SBS org	§10.3

A.6 Software Baseline (As Built)

Docker 29.1.3 / Compose 2.40.3 (prod, dev, monitor) · Grafana 13.1.0 (grafana apt repo) · Prometheus + node_exporter ×4 (Ubuntu repo) · nginx 1.28.3 · certbot + LE cert live on monitor · BookStack (wiki). Pending install: Node LTS/pnpm, Rust/Cargo, Python venvs, PostgreSQL, MongoDB, Redis, Vault, Loki, Alertmanager, blackbox/cAdvisor/engine exporters, oauth2-proxy, AnythingMCP.

Appendix B — Firewall Rule Tables (Target, §3.5–3.6)

B.1 Cloud Firewalls (tag-scoped) — as built: none exist ⚠ (item 19)

FW / tag	Inbound	Outbound
`prod-app` / `prod`	443, 80 ← any · 22 ← monitor private IP only (bastion) · 9100+exporters ← monitor private IP	§3.4 allowlist
`prod-monitor` / `grafana`	443, 80 ← any · 22 ← admin allowlist (sole public SSH into Prod) · [3000/9090/9100 localhost-bound — no rule]	§3.4
`prod-wiki` / `wiki`	443, 80 ← any · 22 ← monitor private IP · 9100 ← monitor private IP	§3.4
`prod-vault` / `vault`	8200 ← prod-app, dev, bastion private IPs · 22 ← monitor private IP	§3.4 (narrow)
`dev-app` / `develop`	22 + web ← admin allowlist only	§3.4 + language registries (build context)

B.2 Host Firewall (nftables target; as built: ufw on monitor/wiki only, none on prod/dev ⚠ item 20)

Baseline: inbound default-deny mirroring Cloud FW; outbound default-deny + allowlist — 443→Anthropic API, GitHub/GHCR, apt mirrors, LE ACME; 123→NTP; 53→DO resolvers. Per-Compartment chains: egress = Anthropic + that Compartment's declared integrations only (§3.4). Ruleset hash exported to `integrity` job (§12.2).

B.3 Egress Allowlist Summary

Destination	Ports	Scope
Anthropic API	443	All prod + per-Compartment chains
GitHub / GHCR	443	Deploy/CI paths
Ubuntu archive/security, grafana apt	443/80	Hosts

Destination	Ports	Scope
registry.npmjs.org, crates.io, pypi.org	443	**Build contexts only — unreachable from prod runtime** (§11.2)
Let's Encrypt ACME	443	Edge hosts
DO resolvers / NTP pool	53 / 123	All

Appendix C — Build Register (Consolidated, items 1–115)

Status: done · ◐ partial · ○ open · blocked/decision · numbering per chapter of origin.

#	Item	Ch.	Status
1–3	DO account; Dev + Prod projects	2	
4	Dedicated VPCs ×2 (10.10/10.20)	3	○ (rebuild wave)
5	Cloud Firewalls ×4(+vault)	3	○
6	Admin SSH allowlist captured in IaC	3	○
7	nftables baseline + Compartment chains	3	○
8	Domain transfer to SBS + lock + registrar MFA	4	◐ (registered; transfer pending)
9	Zone cutover GoDaddy → DNSSEC provider + NS	4	○
10	DS publication + chain verification (AD/DNSViz)	4	○ (after 9)
11–12	Null-mail records; CAA	4	○ — **publishable now (item 23)**
13–14	CT alert subscription; dnstwist weekly	4	○
15	**Credential rotation + Vault migration + changelog purge + SBS-alias identities**	2/8	**CRITICAL — execute §8.6 order**
16	**Apex repoint 138.197.222.154 → prod**	2/4	gated on Ch. 5 prod edge
17	Per-person users, root-SSH disable, sudo scoping	2	○ (via item 60)
18	**VPC rebuild decision (a)/(b)**	3	decision — spec assumes (a)
19	Cloud FW creation	3	○ (=5)
20	Host firewall activation prod/dev (stopgap ufw → nftables)	3	○ urgent
21	OS standardization (24.04 vs 26.04)	2	decision; executes via item 115
22	`Dev-Gitlab-server` disposition	2	decision
23	Publish null-mail + CAA on GoDaddy pre-cutover	4	○ immediate
24–29	Monitor nginx to fleet TLS/header template; social-card stripping; HSTS staged+preload sign-off; expiry probes; prod nginx+certs; admin edge allowlist	5	○

#	Item	Ch.	Status
30–35	Toolchain install+pinning; Compartment compose template+net-edge; container hardening; interim data stacks; MCP sidecar pattern; compose-vs-running drift metric	6	○
36	**NYC2 Managed DB availability check**	7	blocks §7.2 path + item 106
37–41	Data Volumes; per-Compartment DB/role/ACL scripts; internal CA; Spaces buckets+keys; sanitized-dump script	7	○
42–48	Vault droplet+Volume+FW; Shamir ceremony; mounts/policies/AppRoles; DB+PKI engines; deploy-render integration; gitleaks; rotation runbook	8	○
49	**IdP product confirmation (DISC-002)**	9	blocks 50–54
50–56	IdP registrations+groups; oauth2-proxy; Grafana OIDC; BookStack SSO; SCIM+timed test; break-glass ceremony; first IAM-06 review	9	○
57–62	Infra repo+protection+CI; tofu import (nonconformance baseline); rebuild-wave authoring; Ansible base role fleet-wide; drift jobs+induced test; Prod approval gate	10	○ — 58 executes 96-residual; 59 executes 4/18/42; 60 executes 17/20/109
63–70	GHCR+pull token; base-image allowlist+digest lint; frozen-lockfile gates; cosign sign+verify; SBOM; Trivy gate+nightly; Renovate; Actions digest pinning	11	○
71–78	Alertmanager+routes; blackbox ×5; Loki+agents; cAdvisor+engine exporters; integrity metrics; dead-man+external check; dashboard repo graduation; monitoring-role absorption	12	○ (core stack live)
79–85	Audit writer+net-audit+Volume; segment format+signing; Rekor+email anchors; continuous verifier; independent CLI; deletion ceremony+legal hold; drill set	13	○
86–95	Tier-2 dump pipeline; offline age custody; repo mirrors; Vault snapshots; SFO3 replication; age metrics+alert; weekly restore-verify; runbooks; WAL-PITR trigger; drill calendar	14	○
96	DO Backups enablement	14	◐ enabled; residual: plan/frequency audit + tofu codification
97	DO API backup-age → integrity metric	14	○ **prioritized**
98	Monthly backup→snapshot conversion	14	○
99	Plan-type/pricing verification	14	○
100	First tier-1 restore drill	14	○ immediate
101	Gitlab-server pre-repoint backup	14	○ before item 16
102–108	Threshold rules+annotations; OOM metrics; P1 drill; deploy RAM gate; **P2 decision before Compartment #4**; P1–P6 runbooks; quarterly capacity filing	15	○ (106 on 36)
109–115	unattended-upgrades; reboot metric; window calendar; window runbook+annexes; first monthly window; rollback drill; OS-mix via windows	17	○

Critical path: 15 → 20 → 57/58 → 18(a) rebuild wave (4, 19, 42, wiki NYC2) → 60 (17) → Ch. 5 prod edge (28) → 16 apex repoint → 9/10 DNSSEC cutover. Blocking decisions: 18, 21, 22, 36, 49.

Appendix D — Acronym Table

Acronym	Expansion
ACL	Access Control List
ACME	Automatic Certificate Management Environment
AD (flag)	Authenticated Data (DNSSEC)
AOF	Append-Only File (Redis)
API	Application Programming Interface
CA / CAA	Certificate Authority / CA Authorization (DNS record)
CD / CI	Continuous Delivery / Continuous Integration
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CSP	Content Security Policy
CT	Certificate Transparency
CVE	Common Vulnerabilities and Exposures
DMARC / SPF	Domain-based Message Authentication, Reporting & Conformance / Sender Policy Framework
DNS / DNSSEC	Domain Name System / DNS Security Extensions
DO	DigitalOcean
DR	Disaster Recovery
DS	Delegation Signer (DNSSEC record)
ECDSA	Elliptic Curve Digital Signature Algorithm
FCC	Federal Communications Commission
FW	Firewall
GFS	Grandfather-Father-Son (retention)
GHCR	GitHub Container Registry
HSTS	HTTP Strict Transport Security
IaC	Infrastructure as Code
IAM	Identity and Access Management
IdP	Identity Provider
IOPS	Input/Output Operations Per Second

Acronym	Expansion
JCS	JSON Canonicalization Scheme (RFC 8785)
KMS	Key Management Service
KV	Key-Value (Vault store)
LE	Let's Encrypt
LTS	Long-Term Support
MCP	Model Context Protocol
MFA	Multi-Factor Authentication
MX	Mail Exchanger (DNS record)
NS	Nameserver
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OIDC	OpenID Connect
OOM	Out Of Memory
OS	Operating System
OWASP ASVS	Open Worldwide Application Security Project — Application Security Verification Standard
PII	Personally Identifiable Information
PITR	Point-In-Time Recovery
PKCE	Proof Key for Code Exchange
PKI	Public Key Infrastructure
PR	Pull Request
RBAC	Role-Based Access Control
RDB	Redis Database (snapshot format)
RPO / RTO	Recovery Point Objective / Recovery Time Objective
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SBOM	Software Bill of Materials
SCIM	System for Cross-domain Identity Management
SLA	Service Level Agreement
SNI	Server Name Indication
SOX	Sarbanes-Oxley Act
SPDX	Software Package Data Exchange
SSH	Secure Shell

Acronym	Expansion
SSO	Single Sign-On
TDE	Transparent Data Encryption
TLS	Transport Layer Security
TSDB	Time-Series Database
TTL	Time To Live
UID	User Identifier
VPC	Virtual Private Cloud
WAL	Write-Ahead Log (PostgreSQL)

Appendix E — References

Ref	Document	Applied in
[1]	**NIST SP 800-207**, *Zero Trust Architecture*	§1.2, §7.5 (TLS on internal links — private network ≠ trust boundary), §9 (identity-centric access)
[2]	**OWASP ASVS v4.x, Level 2**	§1.2, APP-01 baseline, §5.5 headers, §9 session/auth
[3]	**OWASP LLM Top 10** (incl. LLM01 Prompt Injection)	§3.4 egress-as-exfiltration control, §6.4 MCP scoping (AI-02), §8.3 credential isolation (AI-03)
[4]	**LH-SBS-SEC-001** — Security & Access Control Specification	Controlling baseline, all chapters; reconciliation 41-vs-36 pending
[5]	**LH-SBS-KO-001 V3.2** — Technical Install and Discovery	Master runbook; control-family import
[6]	**LH-SBS-PRE-001** — Pre-Install Prerequisites	Day-0 gates
[7]	**LH-SBS-INST-001** — Install Runbook, gates V1–V22	Verification sections §§2–17
[8]	RFC 7505 (Null MX) · RFC 8785 (JCS) · RFC 8659 (CAA)	§4.4, §13.2, §4.6
[9]	DigitalOcean product documentation — Backups, VPC, Spaces, Managed Databases	§14.2.1, §3.1, §7.2–7.3
[10]	Sigstore (cosign, Rekor) documentation	§11.5, §13.2
[11]	SERVER_CHANGELOG.md	As-built evidence layer (§1.3)