

DevNest Shared Services & Product Dependency Map (v0.9 – “current as-is”)

Owner: Platform Ops (shared)

Last Updated: October 1, 2025

Note in margin: “Mapping is 90% right; some tags are legacy.”

“This doc reflects intended architecture. Automation scopes read from `inventory.yaml` and may diverge in edge cases.”

Product Line	Shared Services Used	Operational Notes
CommerceHub	Edge/WAF, DNS/Discovery, IAM/PAM, CI/CD, NoSQL, Observability	High retry intensity; peak traffic seasonality.
IdentityCore	Edge/WAF, DNS/Discovery, IAM/PAM, CI/CD, NoSQL, Observability	Systemic; failure blocks login + internal recovery.
InsightStream	Edge/WAF (dashboards), DNS/Discovery, IAM/PAM, CI/CD, NoSQL, Observability	Uses NoSQL for real-time counters + alert metadata.
IntegrationsEdge	Edge/WAF, DNS/Discovery, IAM/PAM, CI/CD, NoSQL, Observability	Vendor-heavy; partner SLA enforcement.

Inventory.yaml

Operational note (attached to YAML): *"Inventory file is consumed by dns-refresh, cicd-scope, edge-rollout. Treat tag edits as Tier-0 changes."*

```
services:
  dns-registry:
    owner: platform-ops
    tags: [controlplane.dns, platform.shared, critical.tier0]

  core-nosql:
    owner: platform-data
    endpoint: nosql.internal.devnest
    tags:
      - data.core-nosql
      - platform.shared
      - critical.tier0
      - controlplane.dns # legacy alias, never removed
```

Shared-Service Tags Used by Automation

Standards Table (What Platform Ops intends)

Shared Service	Documented Tag	Scope	Comments
Shared IAM/PAM	controlplane.identity	Global	Workforce IAM + privileged role routing.
CI/CD Automation	controlplane.cicd	Global	App + infra pipelines; "golden path."
Edge + Bot Protection	frontdoor.edge	Global	WAF/CDN/bot rulesets.
DNS & Service Discovery	controlplane.dns	Global	DNS refresh automation targets this scope.
Core NoSQL Datastore	data.core-nosql	Global	Tier-0 data dependency.
Observability Stack	platform.telemetry	Global	Metrics/logs/traces + alerting.

Margin note: "Documented tags above are normative. Actual automation targets are derived from inventory tags."

Inventory Table (What Automation actually reads)

Shared Service	Actual Tags in Inventory	Scope	Comments
Shared IAM/PAM	controlplane.identity , platform.shared , critical.tier0	Global	Correct per standard.
CI/CD Automation	controlplane.cicd , platform.shared , critical.tier1	Global	Correct per standard.
Edge + Bot Protection	frontdoor.edge , platform.shared , critical.tier0	Global	Correct per standard.
DNS & Service Discovery	controlplane.dns , platform.shared , critical.tier0	Global	Correct per standard.
Core NoSQL Datastore	data.core-nosql , platform.shared , critical.tier0 , controlplane.dns (legacy alias)	Global	Mismatch — legacy tag not removed.
Observability Stack	platform.telemetry , platform.shared , critical.tier1	Global	Correct per standard.

Inventory File Changelog (last 12 months)

File: inventory.yaml

Repo: platform-shared-config

Maintainers: "platform-ops@devnest" + "platform-data@devnest" (rotating)

Date	Change	Author	Notes
2024-12-03	Added <code>controlplane.dns</code> tag to <code>core-nosql</code>	Platform Ops contractor	"NoSQL endpoint managed by DNS module; needs inclusion in refresh."
2025-02-18	Split DNS module ownership from NoSQL	Platform Data lead	"NoSQL now owned by platform-data. Remove DNS alias next cleanup."
2025-04-09	Tag cleanup pass	Platform Ops SRE	Removed aliases on non-Tier-0 services only. "Didn't touch NoSQL — too risky for busy season."
2025-06-14	Added <code>critical.tier0</code> tags	Audit remediation	No alias cleanup performed.
2025-09-30	DNS refresh automation updated	Platform Ops	Scope still relies on tag match. No allow-list.
2025-10-22	Incident: DNS refresh touched multiple targets	Postmortem	Action item: "resolve alias drift." Not completed.

Changelog footer: "Tier-0 alias cleanup scheduled for Q1 but repeatedly deferred due to peak load windows."

Known but Unresolved Issues

- Tier-0 scope drift
 - Tag aliasing on Tier-0 services creates hidden blast radius.
- Global automation without guardrails
 - Both CI/CD and DNS refresh rely on tags, not explicit allow-lists.
- NoSQL feeds observability
 - When NoSQL is degraded, monitoring becomes stale or unavailable.
- Edge has no hard bypass
 - Routing failure blocks status page and app access.
- IdentityCore needed for recovery tools
 - SSO outage slows incident response.