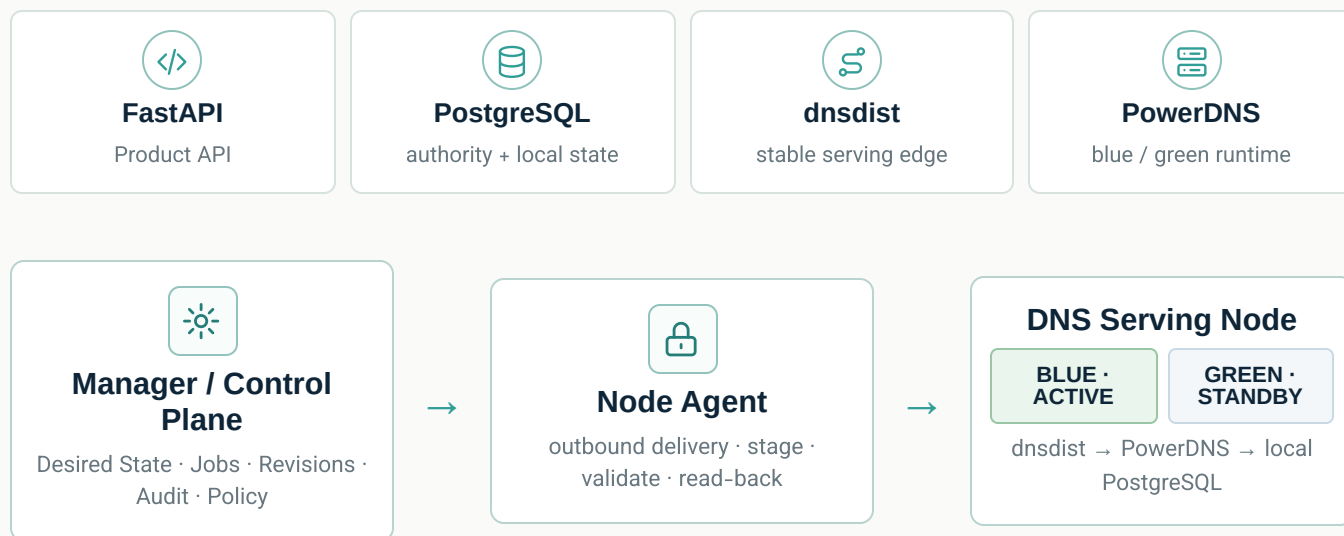


4SO GeoDNS

Authoritative DNS + Global Traffic Management

API-first Control Plane for Desired State, Revision, Delivery, DNSSEC and DNS Node lifecycle, with a Serving Path independent of the Manager and atomic Blue/Green cutover.



Query Path independent of the Manager

A normal DNS query does not depend on a live Manager, a cross-region database or synchronous health HTTP.

Atomic Runtime Delivery

A Revision is first staged and validated on the inactive color; dnsmist then switches the path with an atomic cutover.

Define desired state in the Control Plane; the DNS Node answers from verified local state.

PRODUCT BOUNDARY

One Control Plane, four clear operational boundaries

Authority, delivery, serving and policy are separated so a failure in one layer never blurs the meaning or ownership of the others.

Control Plane Authority

POSTGRESQL

**Desired State**

zone / record / policy / node intent

**Jobs + Revisions**

durable lifecycle and delivery identity

**Audit + Outbox**

mutation history and durable dispatch

Delivery Plane

mTLS

**Worker**

selects nodes by fabric / placement

**Node Agent**

pulls outbound and stages inactive color

**Read-back**

PowerDNS API + local validation before cutover

Serving Plane

LOCAL

**dnsmist**

stable query edge and color selection

**PowerDNS Blue/Green**

active runtime + retained previous healthy color

**Local PostgreSQL**

independent node-local authoritative state

Policy & Security

BOUNDED

**Geo / ASN / CIDR**

deterministic rule priority

**DNSSEC / TSIG**

key, rollover and transfer lifecycle

**Health Snapshot**

computed out of band; query reads local versioned state

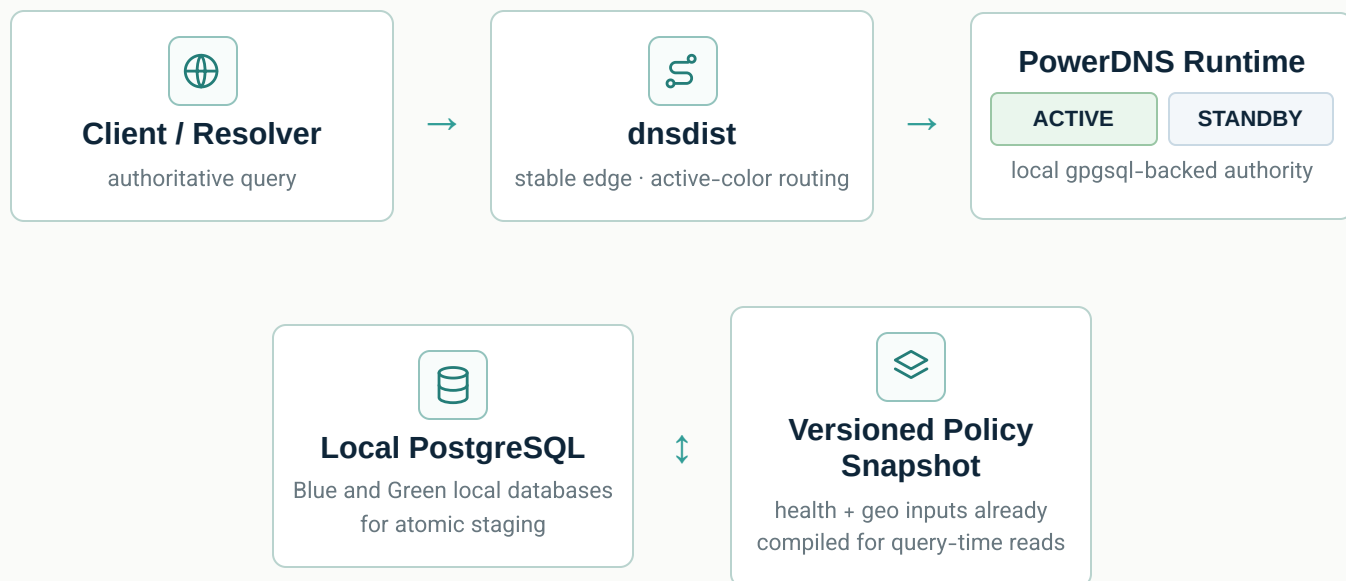


Ownership principle: PostgreSQL holds Control Plane authority; the DNS Node relies on local verified state for serving, not on a live control-plane request.

SERVING ARCHITECTURE

DNS answers pass through the local runtime

The serving path is deliberately short and local; the Manager is not on the synchronous query path.



Manager outage boundary



If the Control Plane is temporarily unavailable, DNS serving continues from verified local state. Desired-state changes pause; query answers must never wait on a synchronous call to the Manager.

Zone data stays authoritative



GeoIP capability is added alongside gpgsql zone authority; zone data is not moved into a GeoIP backend.

No live health HTTP in query

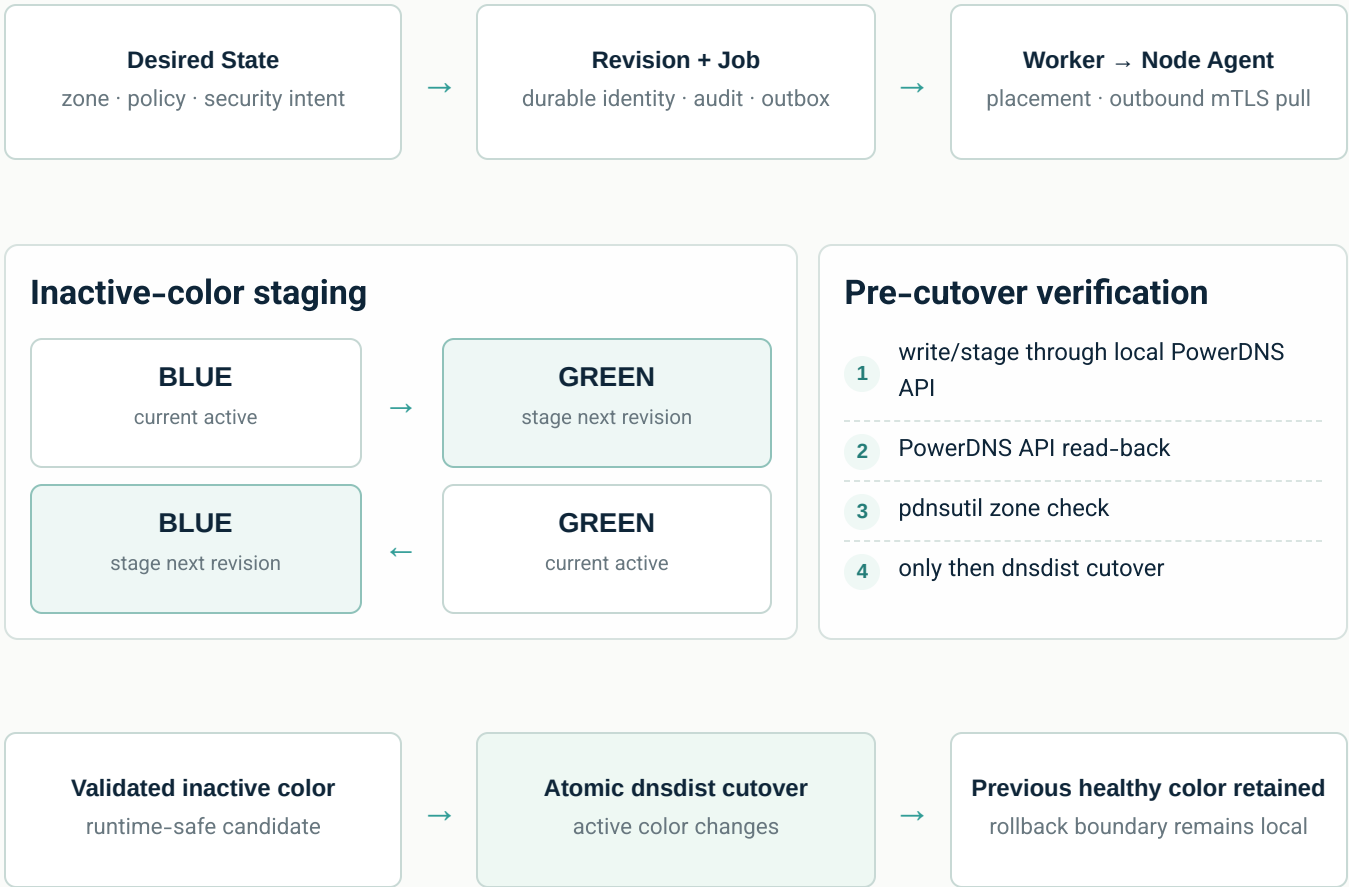


Health is computed out of band; the query reads only a local, versioned snapshot.

REVISION DELIVERY

Stage → Validate → Cut over → Retain

Blue/Green is not just two services with the same name; it is a delivery protocol that genuinely verifies the inactive color before the query path changes.



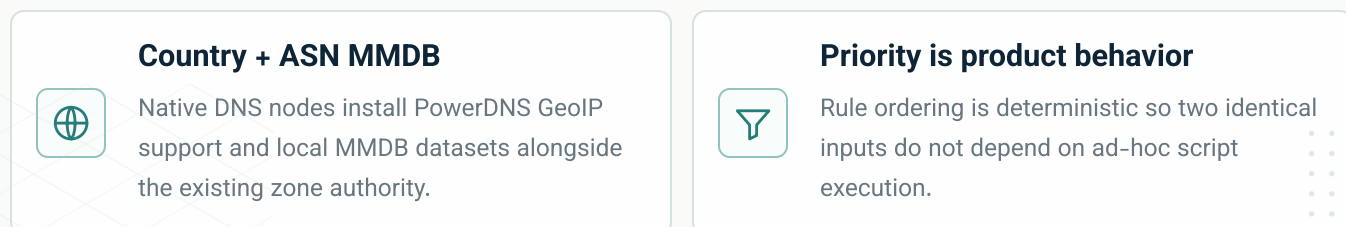
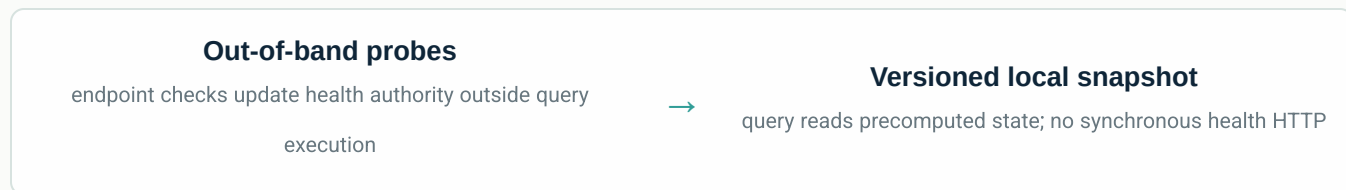
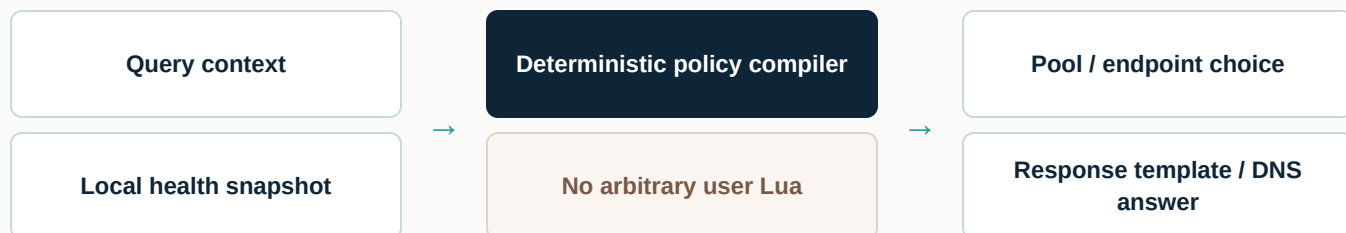
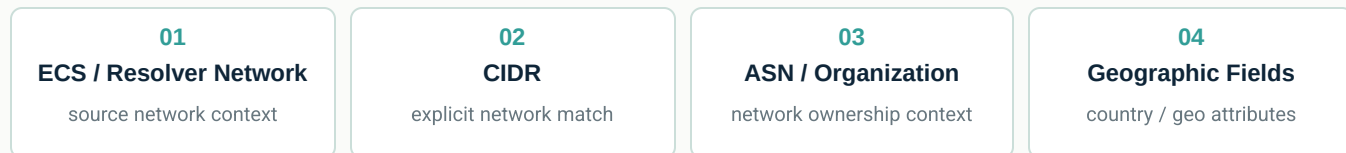
Fail closed before cutover

If read-back or required validation does not pass, cutover must not happen. “revision created” or “stage command returned” alone is not serving success.

TRAFFIC POLICY

Deterministic policy; health stays off the DNS answer path

Geo-routing evaluates network and geographic inputs in a defined order; arbitrary user Lua is not part of the policy compiler.



DNS SECURITY

Security lifecycle alongside the delivery lifecycle

DNSSEC, TSIG and transfer policy are not mere configuration fields; changing them must stay aligned with the revision, validation and cutover of the same serving path.



DNSSEC

Policy + keys

managed as product-owned lifecycle state

Rollover

sequenced change rather than ad-hoc replacement

Pre-cutover validation

inactive runtime checked before serving switch



TSIG & Transfers

TSIG keys

bounded identity for transfer/update paths

Transfer policy

product-owned allow/deny boundary

Secondary / dynamic update

integrated with zone lifecycle rather than bypassing it



Blue / Green safety

Inactive-first mutation

new security state is staged off-path

Read-back + zone check

runtime proof gates cutover

Previous healthy color

retained for local rollback boundary



Audit & Evidence

Durable job identity

change is traceable to a lifecycle operation

Revision identity

what was delivered is explicit

Runtime read-back

success closes on serving evidence

Rollover semantics

Prepare next key/state



Stage inactive color



Validate runtime



Cut over + observe



NODE LIFECYCLE & RECOVERY

From node registration to replacement; the Manager stays off the DNS answer path

DNS Node lifecycle is controlled by jobs and the mTLS agent, while serving continues from verified local state.

Node onboarding

- 01 Register intent / target
- 02 mTLS enrollment / identity
- 03 Install dnsmdist + PowerDNS blue/green + local PostgreSQL
- 04 Runtime attest / health
- 05 Eligible for revision rollout

Day-2 lifecycle

- 01 Drain / undrain
- 02 Fleet rollout by serving fabric / placement
- 03 Replace node with new identity
- 04 Remove node with explicit data-loss boundary
- 05 Reconcile desired vs runtime evidence

Manager reachable

new jobs / revisions continue; nodes pull desired work over mTLS



Manager unavailable

new mutations pause; verified local DNS serving continues

Recovery principle



A control-plane failure must not turn into a simultaneous query-serving failure. Once the Manager returns, reconciliation must re-converge desired state, revision history and runtime read-back.



ACTION & OPERATIONS CATALOG

Control, delivery, serving and recovery in one cycle

CFG

Desired State & Delivery

zone

record

revision

deploy

validate

cutover

rollback boundary

Changes are bound to a revision and runtime verification, never to direct writes on the active serving state.

GTM

Traffic Management

endpoint

pool

probe

health snapshot

GeoIP

ASN

CIDR

The policy compiler turns structured input into an answer choice with deterministic priority.

SEC

DNS Security

DNSSEC

key rollover

TSIG

transfer policy

secondary

dynamic update

Security state follows the same delivery and read-back discipline.

NOD

Node & Recovery

enroll

rotate mTLS

drain

undrain

replace

remove

reconcile

Node lifecycle is managed from the Control Plane; query serving depends on local verified state.

What does this brochure establish?

4SO GeoDNS is not just a UI for DNS records; it is an authoritative DNS lifecycle control plane that connects Desired State, Revision Delivery, Blue/Green serving, Traffic Policy and DNS Security with runtime evidence.

01

Manager ≠ query path

02

dnssdist → PowerDNS
→ local PostgreSQL

03

Blue / Green atomic cutover

04

Deterministic geo policy

05

Out-of-band health snapshot

06

DNSSEC / TSIG lifecycle

Define desired DNS state. Validate the inactive runtime. Cut over atomically.

The architectural goal: DNS changes stay controllable, while serving itself relies on verified local state.