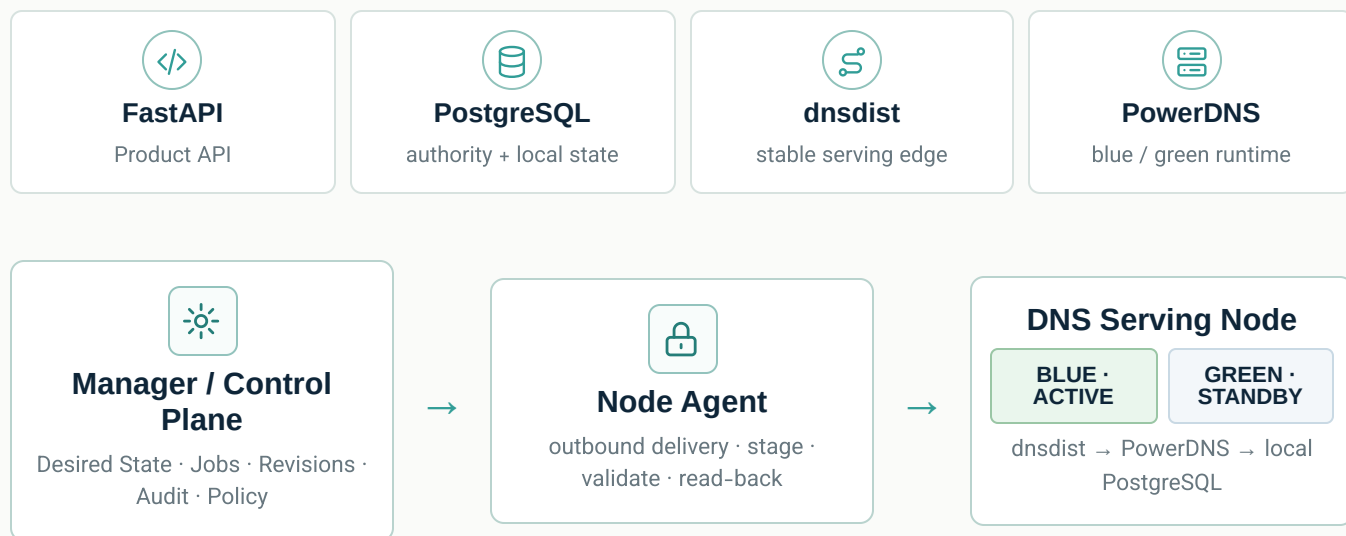


4SO GeoDNS

Authoritative DNS + Global Traffic Management

و Desired State، Revision، Delivery، DNSSEC برای Control Plane API-first
چرخه عمر DNS Node؛ با Serving Path مستقل از Manager و cutover اتمیک
.Blue/Green



Atomic Runtime Delivery

Revision ابتدا روی رنگ غیرفعال stage و validate می‌شود، سپس dnsdist با cutover اتمیک مسیر را تغییر می‌دهد.

Query Path مستقل از Manager

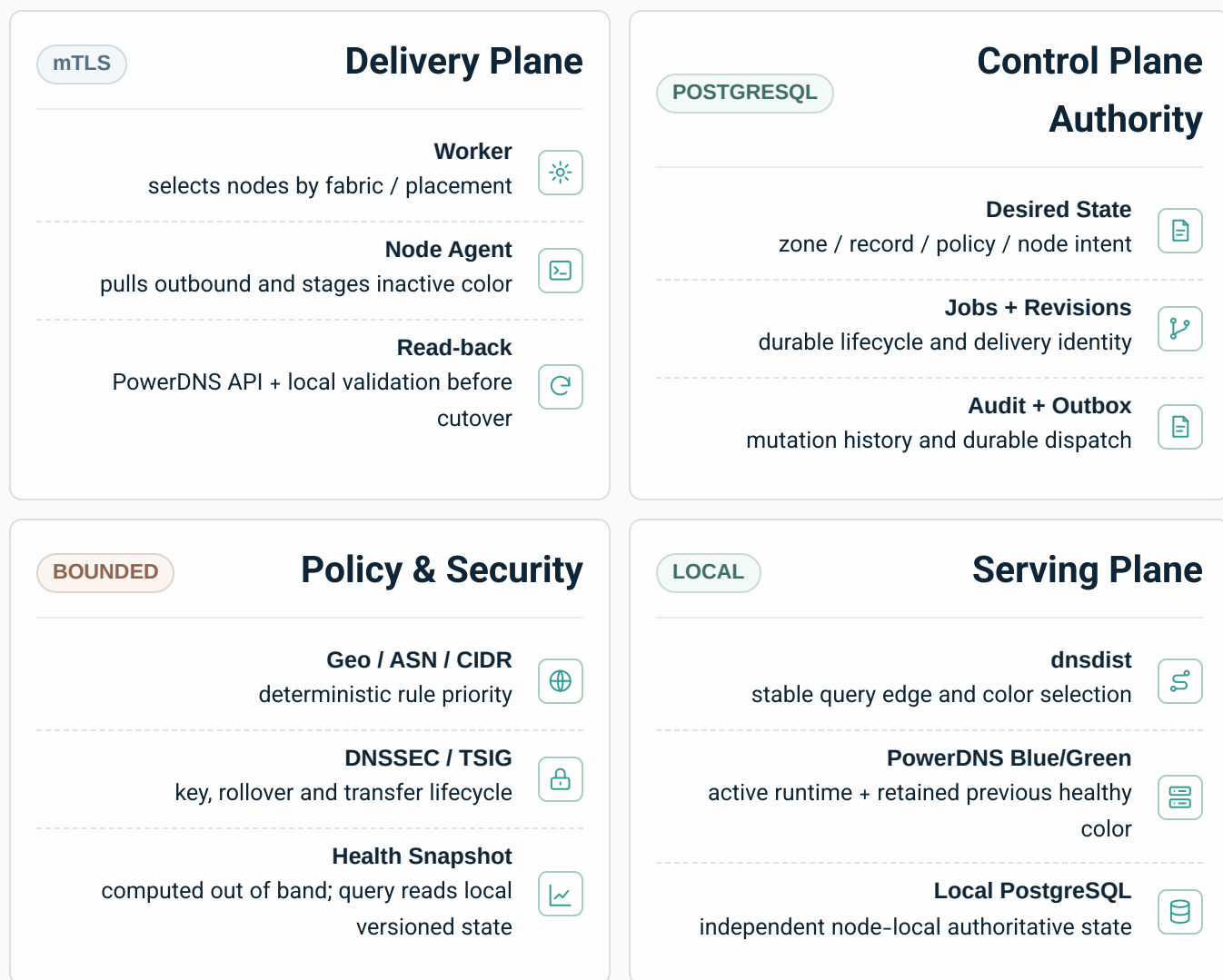
Normal DNS query به Manager زنده، cross-region، database یا HTTP synchronous health وابسته نیست.

Desired state را در Control Plane تعریف کنید؛ DNS Node از verified local state پاسخ می‌دهد.

PRODUCT BOUNDARY

یک Control Plane، چهار مرز عملیاتی روشن

در یک لایه، معنا و ownership لایه‌های دیگر را مبهم نکند. failure و Authority، delivery، serving از هم جدا هستند تا



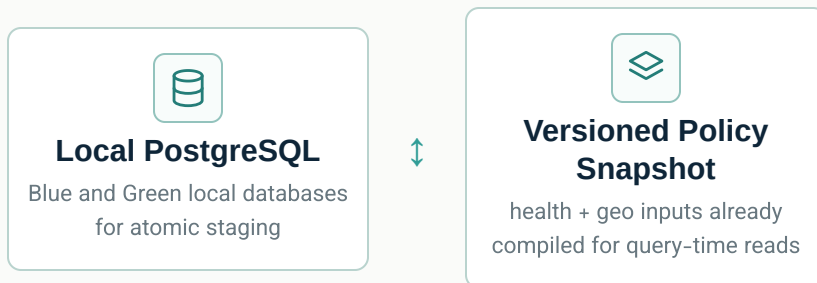
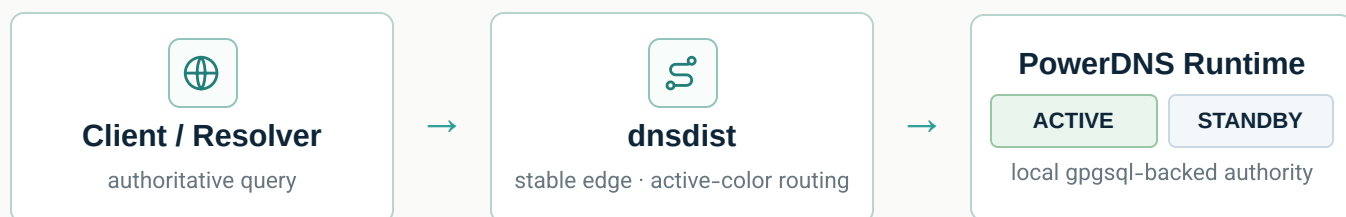
اصل مالکیت: PostgreSQL Control Plane authority را نگه می‌دارد؛ DNS Node برای serving به local verified state تکیه می‌کند، نه به request-control-plane.live.



SERVING ARCHITECTURE

پاسخ DNS از Runtime محلی عبور می‌کند

Serving path عمداً کوتاه و local است؛ Manager در مسیر synchronous query قرار نمی‌گیرد.



Manager outage boundary

اگر Control Plane موقتاً در دسترس نباشد، DNS serving از verified local state ادامه می‌دهد. تغییر desired state متوقف می‌شود؛ پاسخ‌گویی query نباید برای تماس synchronous با Manager منتظر بماند.



No live health HTTP in query

Health out-of-band محاسبه می‌شود؛ query فقط snapshot محلی و versioned را می‌خواند.



Zone data stays authoritative

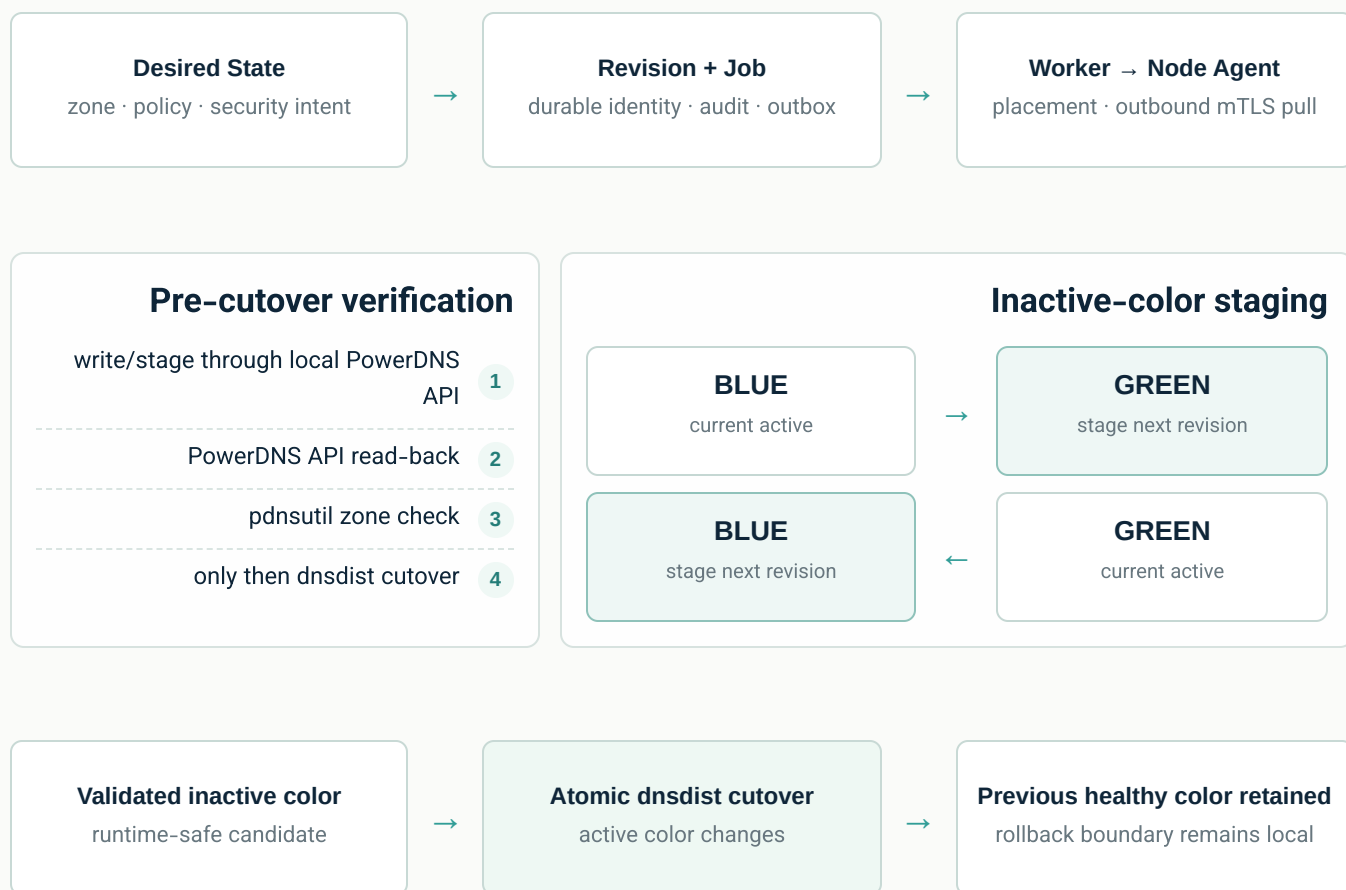
GeolP capability در کنار gpgsql zone authority اضافه می‌شود؛ zone data به GeolP backend منتقل نمی‌شود.



REVISION DELIVERY

Stage → **Validate** → **Cut over** → **Retain**

Blue/Green فقط دو سرویس هم‌نام نیست؛ یک protocol تحویل است که inactive color را پیش از تغییر مسیر query به‌طور واقعی می‌سنجد.

**Fail closed before cutover**

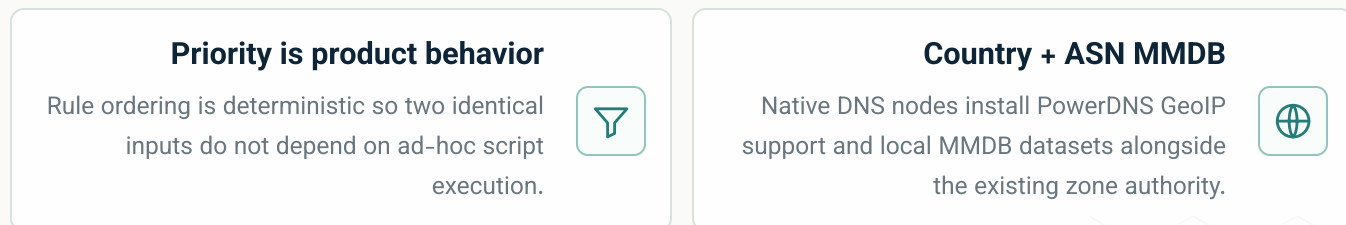
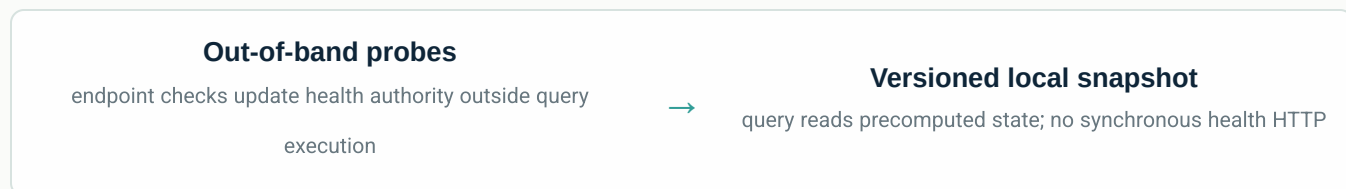
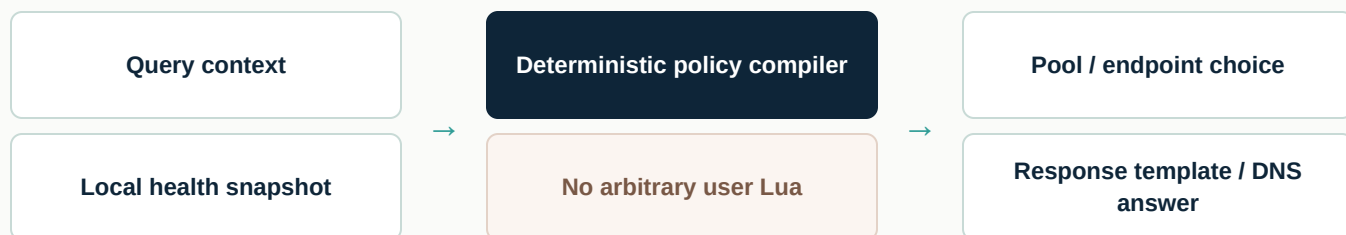
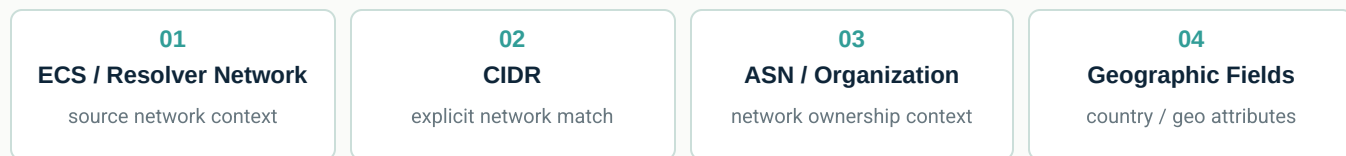
اگر read-back یا required validation پاس نشود، cutover نباید رخ دهد. «revision created» یا «stage command returned» به‌تنهایی success serving نیست.



TRAFFIC POLICY

سیاست قطعی؛ Health خارج از مسیر پاسخ DNS

Geo-routing ورودی‌های شبکه و جغرافیا را با ترتیب مشخص ارزیابی می‌کند؛ arbitrary user Lua بخشی از policy compiler نیست.



DNS SECURITY

delivery lifecycle کنار Security lifecycle

TSIG، DNSSEC، و transfer policy فقط فیلد configuration نیستند؛

تغییر آن‌ها باید با validation، revision، و cutover همان serving

path هم‌راستا باشد.

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

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

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

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

Rollover semantics

Prepare next
key/state



Stage inactive color



Validate runtime



Cut over + observe

NODE LIFECYCLE & RECOVERY

از ثبت نود تا جایگزینی؛ Manager خارج از مسیر پاسخ DNS

DNS Node lifecycle با job و mTLS agent کنترل می‌شود، اما serving از verified local state ادامه دارد.

Day-2 lifecycle

Drain / undrain 01

Fleet rollout by serving fabric / placement 02

Replace node with new identity 03

Remove node with explicit data-loss boundary 04

Reconcile desired vs runtime evidence 05

Node onboarding

Register intent / target 01

mTLS enrollment / identity 02

Install dnsmdist + PowerDNS blue/green + local PostgreSQL 03

Runtime attest / health 04

Eligible for revision rollout 05

Manager reachable

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



Manager unavailable

new mutations pause; verified local DNS serving continues

Recovery principle

Control-plane failure نباید query serving را به یک failure همزمان تبدیل کند. پس از بازگشت Manager، reconciliation باید revision history و desired state، runtime read-back را دوباره همگرا کند.



ACTION & OPERATIONS CATALOG

کنترل، تحویل، پاسخ‌گویی و بازیابی در یک چرخه

Traffic Management GTM

endpoint pool probe health snapshot GeoIP
ASN CIDR

deterministic Policy compiler ورودی structured را با اولویت deterministic به انتخاب پاسخ تبدیل می‌کند.

Desired State & Delivery CFG

zone record revision deploy validate
cutover rollback boundary

تغییرات به revision و runtime verification وصل می‌شوند؛ نه به نوشتن مستقیم روی active serving state.

Node & Recovery NOD

enroll rotate mTLS drain undrain replace
remove reconcile

query از Node lifecycle از Control Plane مدیریت می‌شود؛ serving به local verified state وابسته است.

DNS Security SEC

DNSSEC key rollover TSIG transfer policy
secondary dynamic update

Security state همان discipline تحویل و read-back را دنبال می‌کند.

dnsmasq → PowerDNS
→ local PostgreSQL **02**

Manager ≠ query path **01**

Deterministic geo
policy **04**

Blue / Green atomic
cutover **03**

DNSSEC / TSIG
lifecycle **06**

Out-of-band health
snapshot **05**

این brochure چه چیزی را ثابت می‌کند؟

4SO GeoDNS فقط یک UI برای رکورد DNS نیست؛ یک authoritative DNS lifecycle control plane است که Desired State، Revision Delivery، Blue/Green serving، Traffic Policy و DNS Security را با runtime evidence به هم متصل می‌کند.

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

هدف معماری این است که تغییرات DNS قابل کنترل باشند و خود serving به verified local state تکیه کند.

