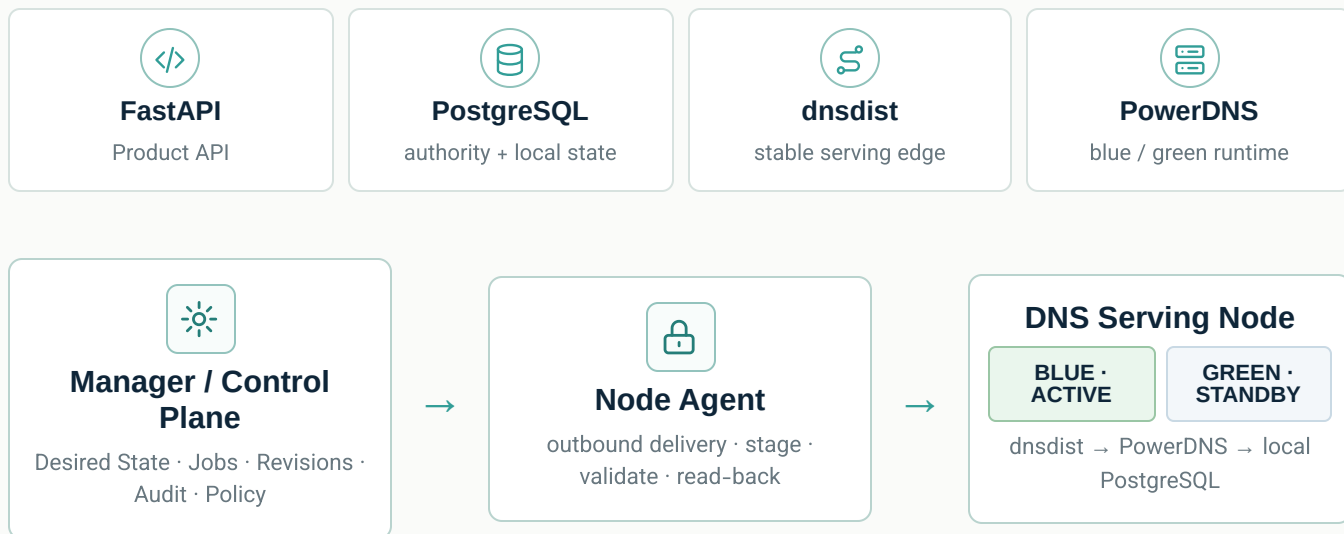


4SO GeoDNS

Authoritative DNS + Global Traffic Management

Control Plane بنهج API-first لـ Desired State و Revision و Delivery
 و DNSSEC و دورة حياة DNS Node؛ مع Serving Path مستقل عن Manager
 و cutover ذري بنمط Blue/Green.



Atomic Runtime Delivery

تُجهَّز Revision أولاً (stage) و يُتحقق منها (validate) على اللون غير النشط، ثم يغيّر dnsdist المسار عبر cutover ذري.

Query Path مستقل عن Manager

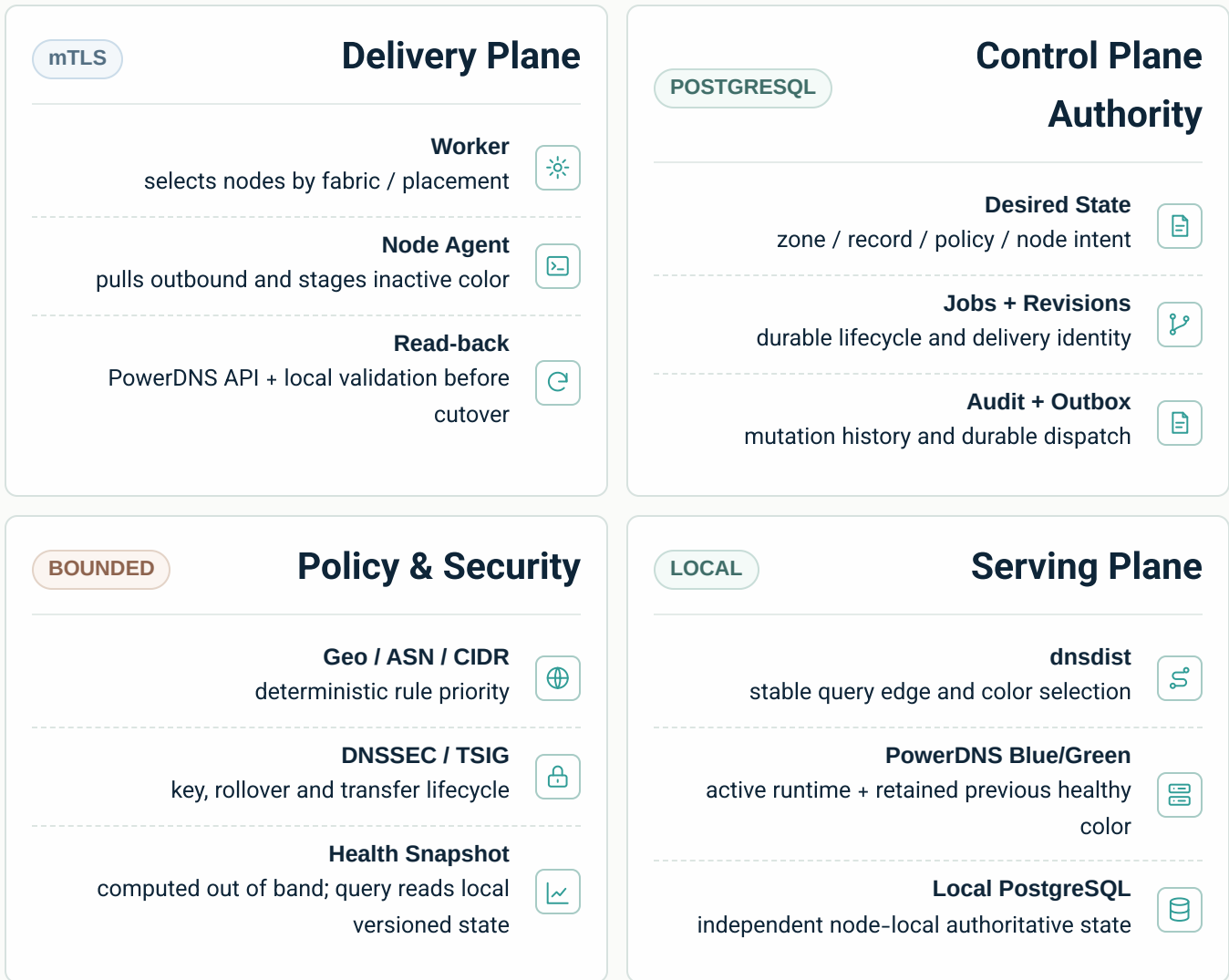
لا يعتمد استعلام DNS العادي على Manager حيّ أو قاعدة بيانات عابرة للمناطق أو HTTP health مترامن.

عرّف الحالة المطلوبة (Desired State) في Control Plane؛ وتجب DNS
 Node من حالة محلية مُتحقّق منها.

PRODUCT BOUNDARY

Control Plane واحد، وأربعة حدود تشغيلية واضحة

تُفصل Authority والتسليم والخدمة والسياسة بعضها عن بعض، حتى لا يُربك عطلٌ في طبقة واحدة معنى الطبقات الأخرى وملكيّتها.



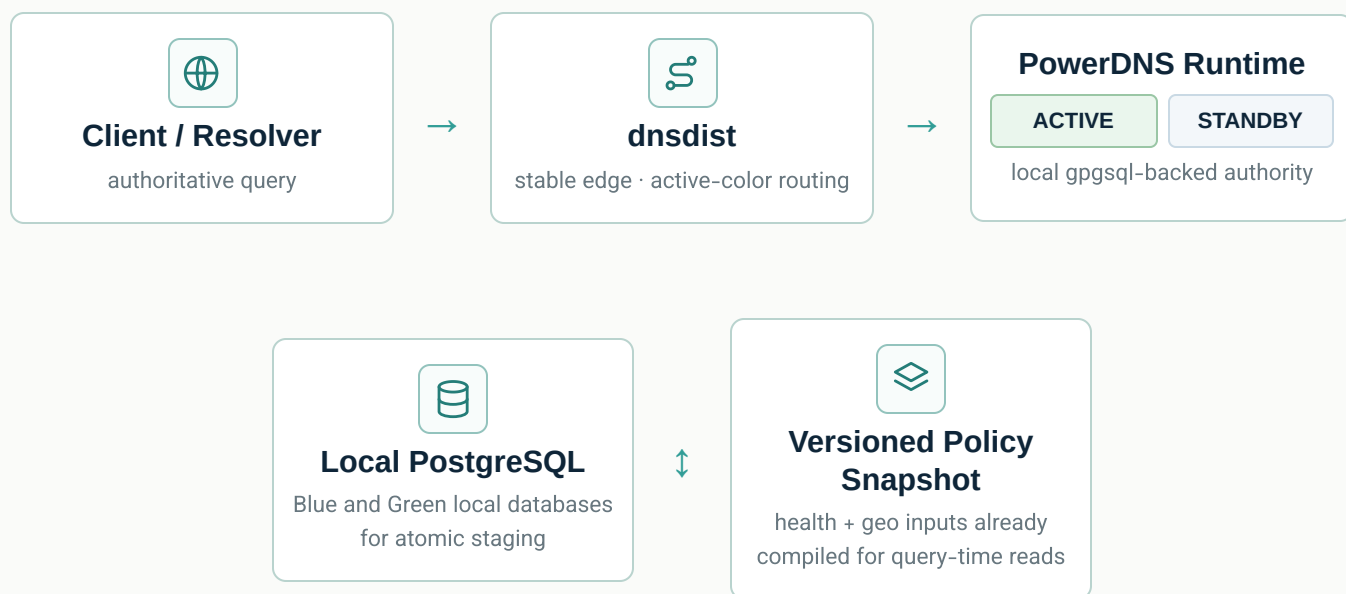
مبدأ الملكية: يحتفظ PostgreSQL بمرجعية Control Plane (authority)؛ وتعتمد DNS Node في الخدمة على حالة محلية مُتحقق منها، لا على طلب حيٍّ إلى Control Plane.



SERVING ARCHITECTURE

إجابة DNS تمر عبر Runtime المحلي

Serving path قصير ومحلي وعمداً؛ ولا يقع Manager على مسار الاستعلام المتزامن.



Manager outage boundary

إذا تعذر الوصول إلى Control Plane مؤقتاً، تستمر خدمة DNS من الحالة المحلية المُتحقق منها. يتوقف تغيير الحالة المطلوبة؛ ولا يجوز أن تنتظر الإجابة على الاستعلام اتصالاً متزامناً مع Manager.



No live health HTTP in query

تُحسب Health خارج مسار الاستعلام (out-of-band)؛ ولا يقرأ الاستعلام إلا snapshot محلية ذات إصدار.



Zone data stays authoritative

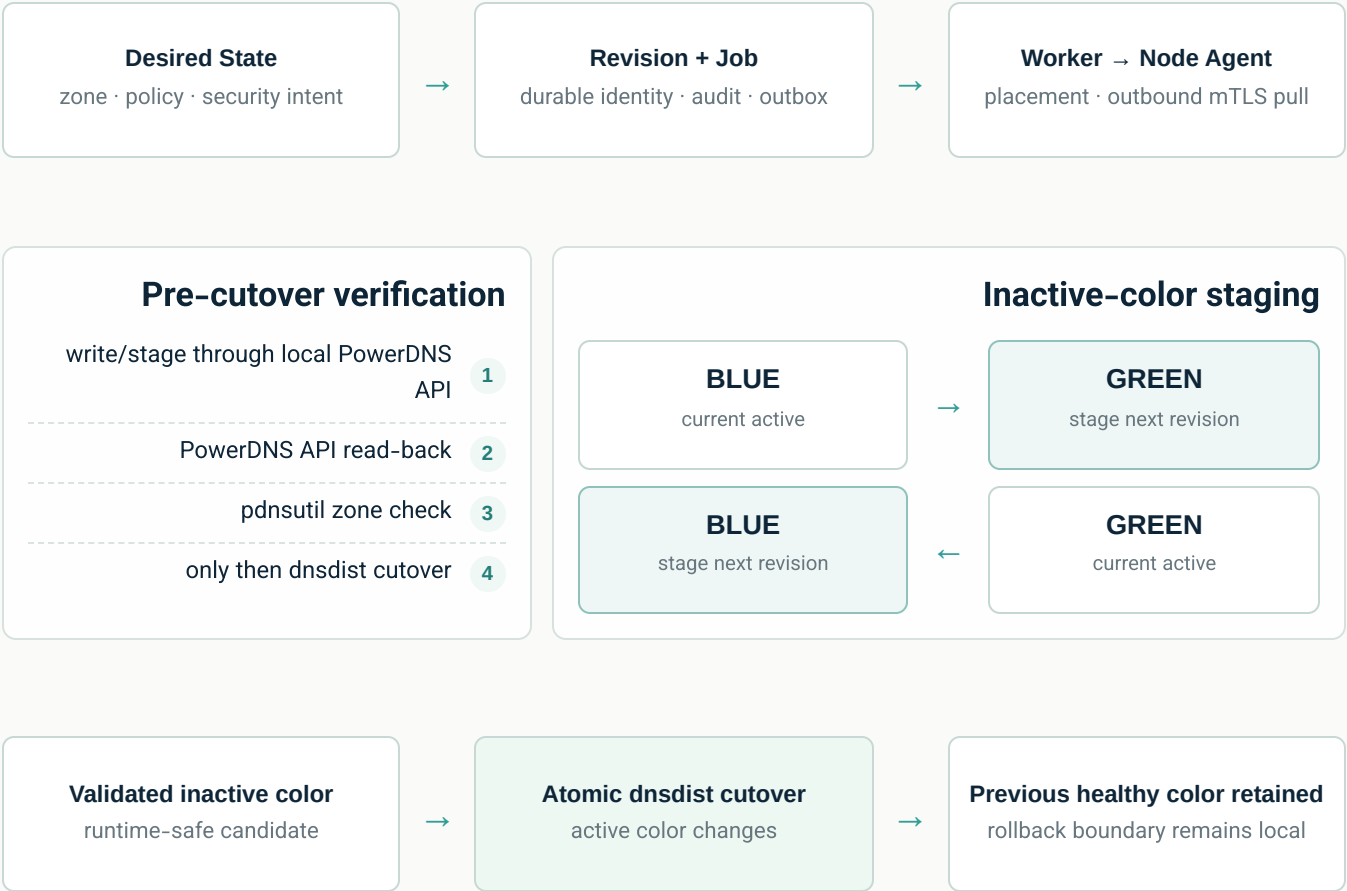
تُضاف GeoIP capability إلى جانب gpgsql zone authority؛ ولا تُنقل zone data إلى GeoIP backend.



REVISION DELIVERY

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

ليس Blue/Green مجرد خدمتين بالاسم نفسه؛ بل هو بروتوكول تسليم يختبر اللون غير النشط فعلياً قبل تغيير مسار الاستعلام.



Fail closed before cutover

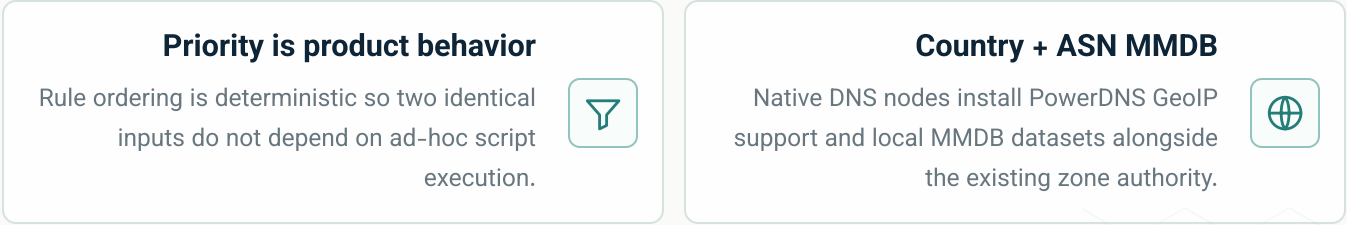
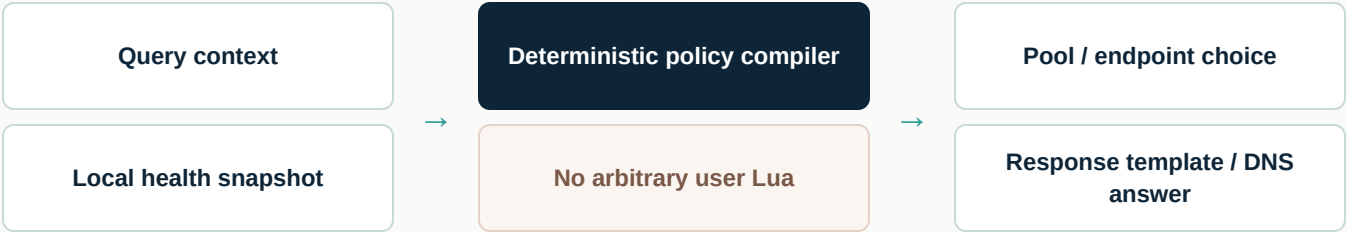
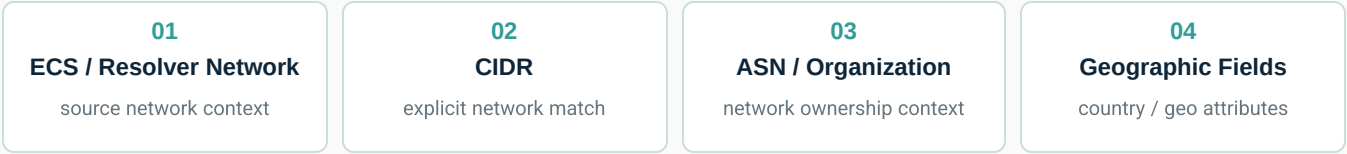
إذا لم ينجح read-back أو التحقق المطلوب، يجب ألا يحدث cutover. ولا تُعدّ عبارة «revision created» أو «stage command returned» وحدها نجاحاً في الخدمة.



TRAFFIC POLICY

سياسة حتمية؛ وHealth خارج مسار إجابة DNS

يقيّم Geo-routing مدخلات الشبكة والجغرافيا بترتيب محدد؛ وليس arbitrary user Lua جزءاً من policy compiler.



DNS SECURITY

Security lifecycle إلى جانب delivery lifecycle

ليست DNSSEC و TSIG و transfer policy مجرد حقول configuration؛ إذ يجب أن يتوافق تغييرها مع revision و validation و cutover لمسار serving نفسه.

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

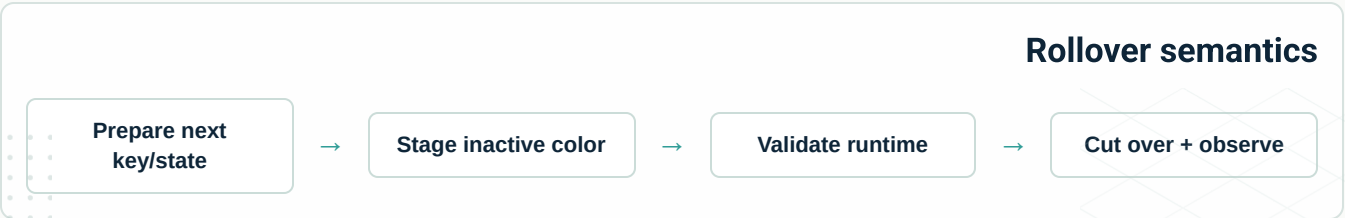
new security state is staged off-path

Read-back + zone check

runtime proof gates cutover

Previous healthy color

retained for local rollback boundary



NODE LIFECYCLE & RECOVERY

من تسجيل العقدة إلى استبدالها؛ وManager خارج مسار إجابة DNS

يُتحكَّم في دورة حياة DNS Node عبر job وmTLS agent، بينما تستمر الخدمة من حالة محلية مُتحقَّق منها.

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

يجب ألا يتحول عطل Control Plane إلى عطل متزامن في خدمة الاستعلامات. وبعد عودة Manager، يجب أن تعيد عملية reconciliation مواءمة الحالة المطلوبة وسجل revision وruntime read-back.



ACTION & OPERATIONS CATALOG

التحكم والتسليم والإجابة والاستعادة في دورة واحدة

Traffic Management GTM

endpoint pool probe health snapshot GeoIP
ASN CIDR

يحوّل Policy compiler المدخلات المهيكلّة إلى اختيار الإجابة وفق أولوية حتمية.

Desired State & Delivery CFG

zone record revision deploy validate
cutover rollback boundary

ترتبط التغييرات بـ revision وبالتحقق في runtime؛ لا بالكتابة المباشرة على حالة الخدمة النشطة.

Node & Recovery NOD

enroll rotate mTLS drain undrain replace
remove reconcile

تُدار دورة حياة العقدة من Control Plane؛ وتعتمد خدمة الاستعلامات على حالة محلية مُتحقّق منها.

DNS Security SEC

DNSSEC key rollover TSIG transfer policy
secondary dynamic update

تتبع حالة الأمان انضباط التسليم و read-back نفسه.

ماذا يُثبت هذا الكتيب؟

ليس 4SO GeoDNS مجرد واجهة لسجلات DNS؛ بل هو مستوى تحكم لدورة حياة Authoritative DNS، يربط الحالة المطلوبة وتسليم Revision وخدمة Blue/Green و Traffic Policy و DNS Security بأدلة runtime.

dnsmist → 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**

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

الهدف المعماري أن تبقى تغييرات DNS قابلة للتحكم، وأن تعتمد الخدمة نفسها على حالة محلية مُتحقّق منها.

