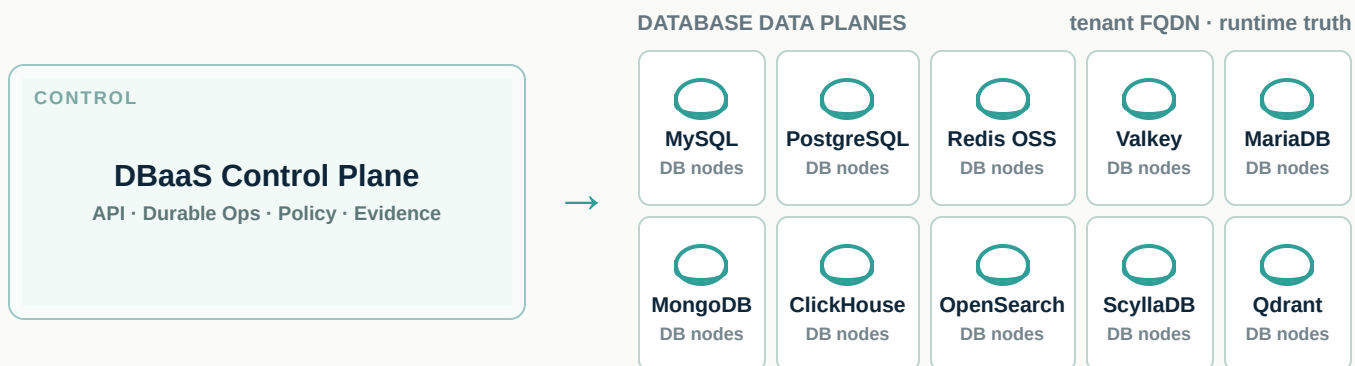
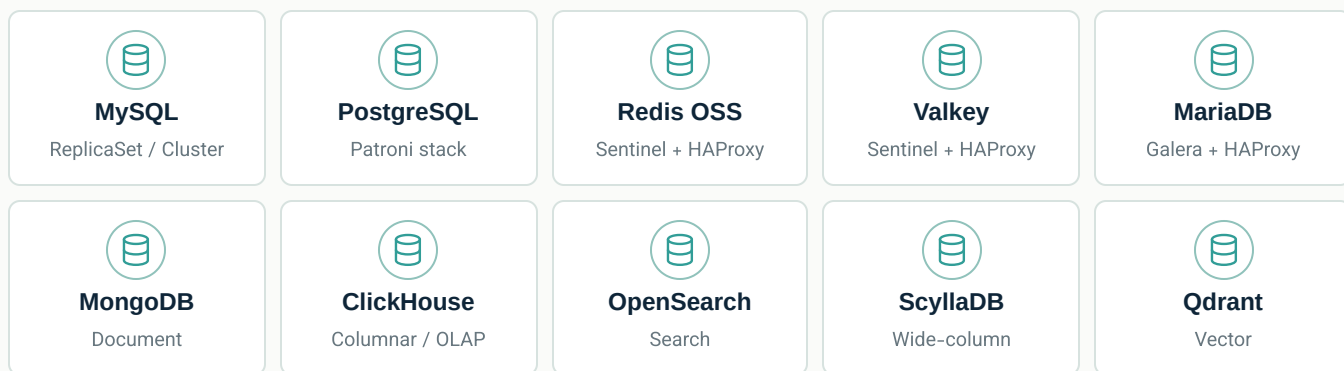


DBaaS Enterprise

التحكم في دورة حياة قاعدة البيانات، لا تثبيتها فقط

عشرة محركات قواعد بيانات تحت Control Plane مشترك لكنه Engine-aware؛ مستوى تحكم مستقل للإطلاق وتغيير السعة والصيانة والاستعادة وقابلية الملاحظة لقواعد البيانات، مع عمليات دائمة وGuardrails للطوبولوجيا وRead-back من Runtime.



النجاح عبر Runtime Read-back
قبول الطلب لا يعني انتهاء العمل؛ يجب تأكيد حالة التنفيذ من Evidence و Runtime.

حدّ واضح بين Control Plane و Data Plane
الـ Manager ليس عضوًا في tenant topology ولا في quorum ولا في مسار خدمة قاعدة البيانات.

قدّم الخوادم والمحرك؛ وتحوّل المنصة دورة الحياة التشغيلية إلى تجربة قابلة للتكرار.



CAPABILITIES SNAPSHOT

نظرة عامة على القدرات



نموذج المنصة

مدخل واحد لنموذج Resource والعمليات	Product API	
PostgreSQL State وDurable Operation في Authority واحدة	PostgreSQL Authority	
RabbitMQ/Celery وTransactional outbox	Outbox + Queue	
إغلاق العمليات بـEvidence والحالة الفعلية	Runtime Read-back	



المحركات والطوبولوجيا

Group ReplicaSet بعقدة/عقدتين، Replication بثلاث عقد	MySQL	
Patroni + etcd + PgBouncer + HAProxy	PostgreSQL	
Replication + Sentinel + HAProxy	Redis OSS / Valkey	
Galera multi-primary + HAProxy	MariaDB	
OpenSearch وClickHouse وMongoDB وQdrant بدلالات أصلية لكل محرك	+5 Engines	



Guardrails التشغيلية

كل action مرتبط بالطوبولوجيا وengine semantics	Topology-aware	
ملكية التنفيذ الدائم ومنع التعارض	Execution Lease	
التنفيذ مقابل source محدد وقابل للإثبات	Source Manifest Fence	
نتيجة job-scoped وread-back تشغيلي	Evidence	



دورة الحياة

Admission والشروط المسبقة وتنفيذ bounded	Provision / Validate	01
تغيير السعة والإصدار مع topology awareness	Scale / Upgrade	02
فقط في الطوبولوجيات التي تستوفي شروط HA	Failover / Recover	03
استعادة مع verify قبل عودة الخدمة	Backup / Restore	04

هدف التصميم: Control Plane مشترك لتجربة تشغيلية موحّدة، دون فرض توحيد semantics المحركات المختلفة.



TOPOLOGY & TRANSITION MATRIX

الطوبولوجيا وQuorum ومسارات تغيير السعة

عدد العقد وحده لا يعني HA؛ دلالات كل محرك تحدد أي العمليات مسموح بها وأي المسارات مقيدة عمداً.

Engine	1 Node	2 Nodes	3 Nodes	HA / Failover semantics
MySQL	ReplicaSet	ReplicaSet	Cluster / GR	HA at 3 data members
PostgreSQL	Patroni	quorum-limited	Patroni HA	etcd + leader election
Redis OSS	single	auto-FO disabled	Sentinel HA	Sentinel-managed
Valkey	single	auto-FO disabled	Sentinel HA	Sentinel-managed
MariaDB	single	no quorum HA	Galera quorum	multi-primary

وثائقي، عمودي/تحليلي، بحث، Wide-column ومتجهي؛ الطوبولوجيا وHA و Data Protection بدلالات المحرك الأصلية نفسها، تحت Control Plane ودورة الحياة ذاتهما. MongoDB · ClickHouse · OpenSearch · ScyllaDB · Qdrant

مسارات تغيير السعة



Stable identity مستقلة عن العقد

هوية العميل هي tenant FQDN؛ يشير مسار الخدمة إلى role النشط ولا يدخل الـ Manager مسار بيانات tenant.

HA action فقط مع طوبولوجيا مناسبة

لا يُعرض Failover التلقائي أو أي action حساس لـ quorum بشكل تزييني على طوبولوجيا تفتقد الأغلبية؛ يقيده الـ Guardrail.

يُغلق الـ Transition عبر Runtime Read-back

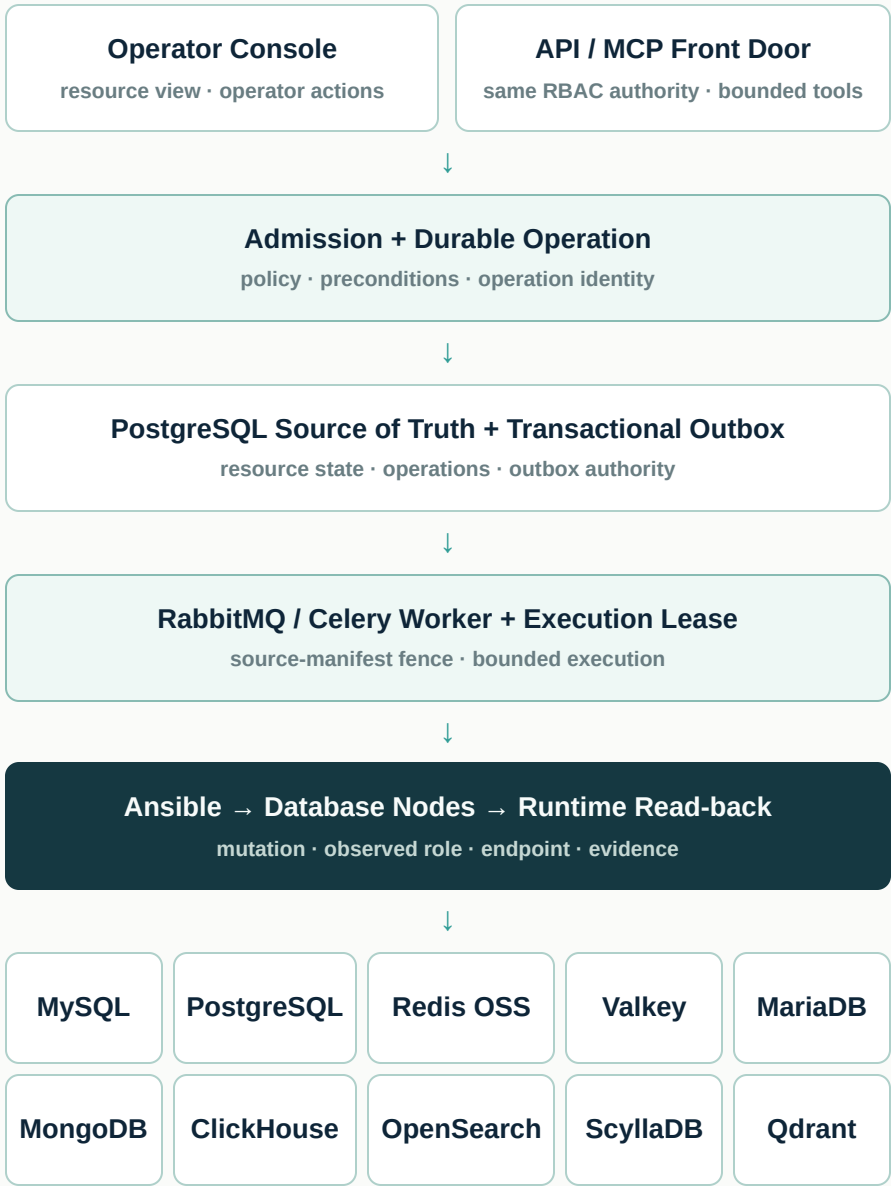
بعد scale أو failover تُقرأ membership و role endpoint من Runtime مجدداً وتُربط النتيجة بالـ operation.

الـ Manager هو Control Plane فقط

الـ Manager ليس witness ولا عضو quorum ولا الـ Router/HAProxy للـ tenant ولا هدف failover.

ARCHITECTURE OVERVIEW

معمارية Control Plane والتنفيذ الدائم



01 Authority واحدة

تعمل Console و API و worker على Resource/Operation authority نفسها؛ ولا تبني الواجهة مصدر حقيقة مستقلاً.

02 الـ Data Plane منفصل

دور Control Plane إداري، وليس عضوًا في replication أو quorum أو tenant service path.

03 التنفيذ fenced

يمنع Lease و source-manifest fence التنفيذ المكرر أو تنفيذ mutation على مدخل خاطئ.

04 الـ Evidence يغلق النتيجة

لا يأتي success من status الداخلي للـ job وحده؛ تُربط runtime state و post-check بالنتيجة.

05 Remote MCP لا ينشئ

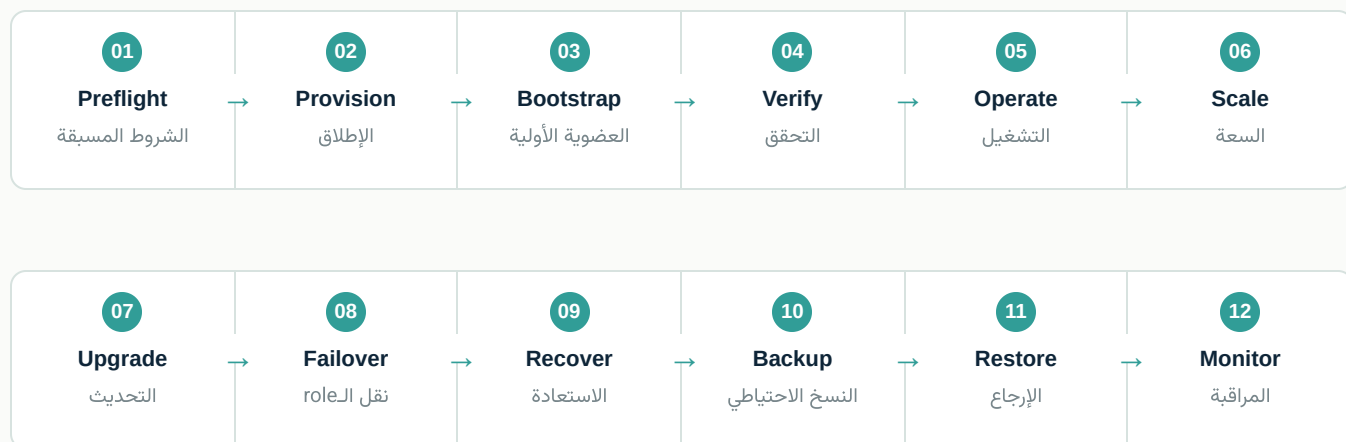
نموذج RBAC جديدًا OAuth 2.1 + PKCE هو المدخل؛ وتبقى authority الصلاحيات هي نموذج PostgreSQL القائم.

Mutation path: Admission → PostgreSQL Durable Operation → Transactional Outbox → RabbitMQ/Celery → Lease/Fence → Ansible → Runtime Read-back → Job-scoped Evidence

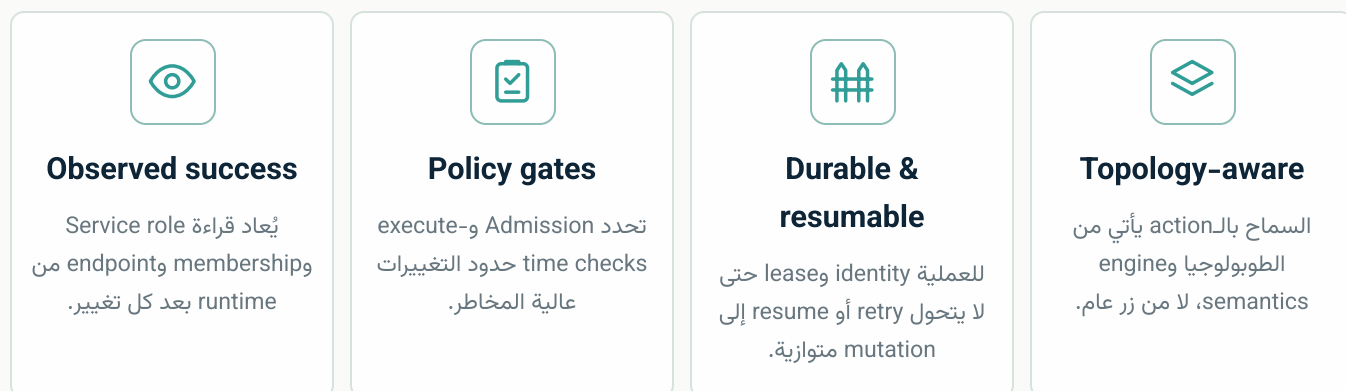
LIFECYCLE OPERATIONS

دورة عمليات قاعدة البيانات الكاملة

الـ Actions ليست مجموعة commands مستقلة؛ لكل تغيير مسار محدد من Admission حتى read-back و recovery.



Guardrails الأساسية



Auditable

Observable

Topology-aware

Repeatable

ENGINE PROFILES

كل Engine يحتفظ بمعماريته الخاصة

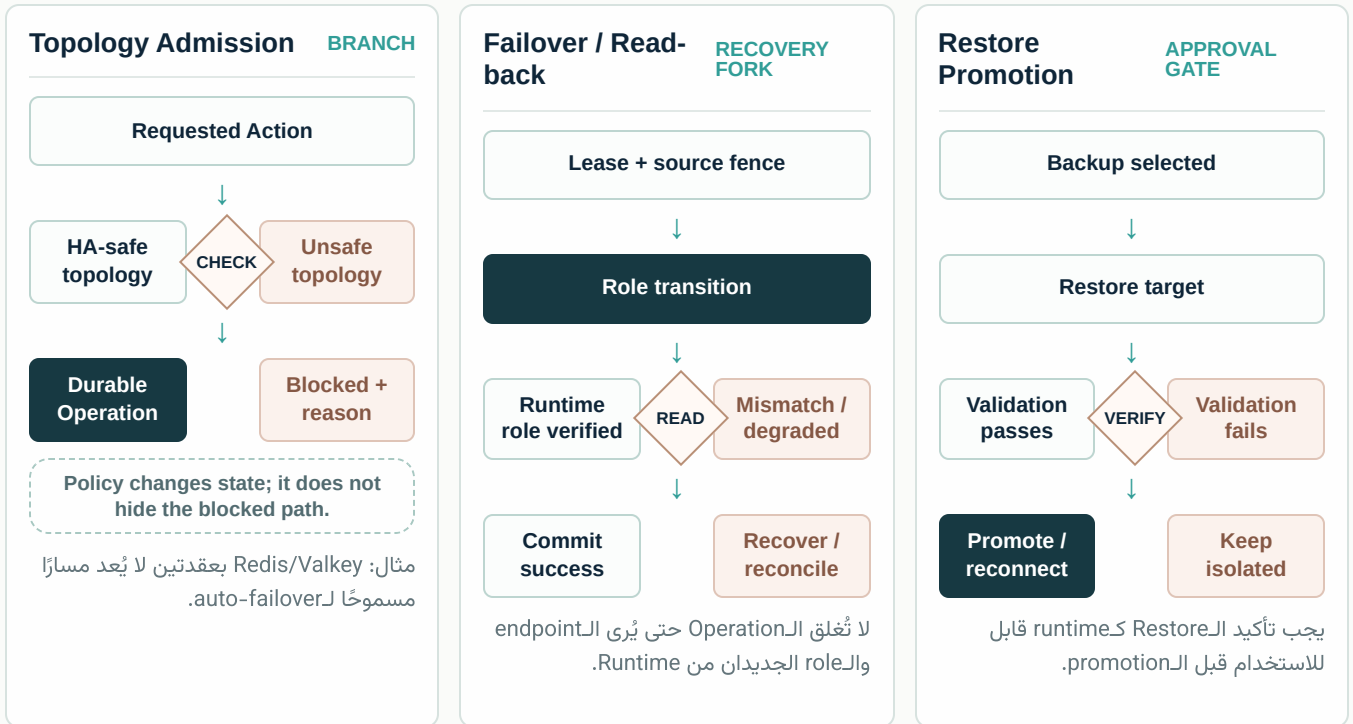
MY MySQL	InnoDB ReplicaSet → InnoDB Cluster / Group Replication 1 / 2 / 3 nodes Routing MySQL Router on DB nodes HA 3-member Group Replication Provision Scale Upgrade Failover Backup Restore
PG PostgreSQL	Patroni + Streaming Replication + etcd + PgBouncer + HAProxy database-node colocated HA stack Leader Patroni / etcd Routing HAProxy + PgBouncer Provision Scale Switchover Backup Restore Monitor
RD Redis OSS	Replication + Sentinel + HAProxy 2-node auto failover disabled Election Sentinel at HA topology Routing HAProxy follows active master Provision Scale Failover Backup Restore
VK Valkey	Replication + Sentinel + HAProxy same safety boundary as Redis Election Sentinel-managed at HA topology 2 nodes automatic failover disabled Provision Scale Failover Backup Restore
MA MariaDB	Galera (wsrep) + HAProxy multi-primary · quorum at 3 members Replication Galera / wsrep Routing HAProxy on DB nodes Provision Scale Upgrade Backup Restore

MongoDB Document	ClickHouse Columnar / OLAP	OpenSearch Search	ScyllaDB Wide-column	Qdrant Vector
---	---	--	---	--

DEEP TECH WORKFLOWS

ثلاثة مسارات ليست «بطاقات خطية»

Gate والfork والreconciliation جزء من المعنى لا زينة. لكل مسار failure/recovery boundary محدد.



المبدأ المشترك

يجب أن يبقى Action catalog واعيًا بالمحرك؛ اسم الـ action وحده لا يعني أنه مسموح على كل الطوبولوجيات.

Action families

- Provision
- Validate
- Scale
- Upgrade
- Switchover
- Failover
- Backup
- Restore
- Monitor
- Diagnose
- Credential lifecycle
- Endpoint read-back

ACTION & OPERATIONS CATALOG

العمليات والأمن والأدلة والاستعادة

Lifecycle & Capacity

L/C

provision scale-out scale-in upgrade restart
rejoin destructive guard

يُغلق تغيير السعة أو العضوية بـ lease و engine semantics
و post-check.

Discovery & Validation

D/V

preflight validate-access runtime-status
primary/role endpoint-status config-check drift

الهدف: أن تكون الطوبولوجيا و runtime truth قابلة للملاحظة قبل
الـ mutation وبعده.

Identity, Access & MCP

SEC

RBAC credential lifecycle OAuth 2.1 PKCE
mcp_clients bounded tools

MCP مدخل آخر إلى الـ authority القائمة؛ ولا ينشئ نموذج
صلاحيات ثانيًا مستقلاً.

HA & Recovery

HA

switchover failover backup restore recover
topology gate

تُحظر عمليات HA على طوبولوجيا غير مناسبة أو تُقَيَّد بدلاً من
تنفيذها «best effort».

ماذا يثبت هذا الكتيب؟

DBaaS ليس installer لعدة محركات؛ بل lifecycle control
plane يحافظ على اختلافات الـ engines ويجعل في الوقت نفسه
Evidence و Policy و Durable Ops مشتركة.

engine profiles 10 02

Control Plane ≠ Data
Plane 01

Runtime read-back 04

Topology-aware
actions 03

Evidence-linked
operations 06

Durable / fenced
execution 05

Choose the engine. Define the topology. Operate the lifecycle.

هدف المنتج ليس إلغاء الخبرة؛ بل تحويل المسارات التشغيلية الحساسة إلى workflows شفافة وقابلة للتكرار والملاحظة.