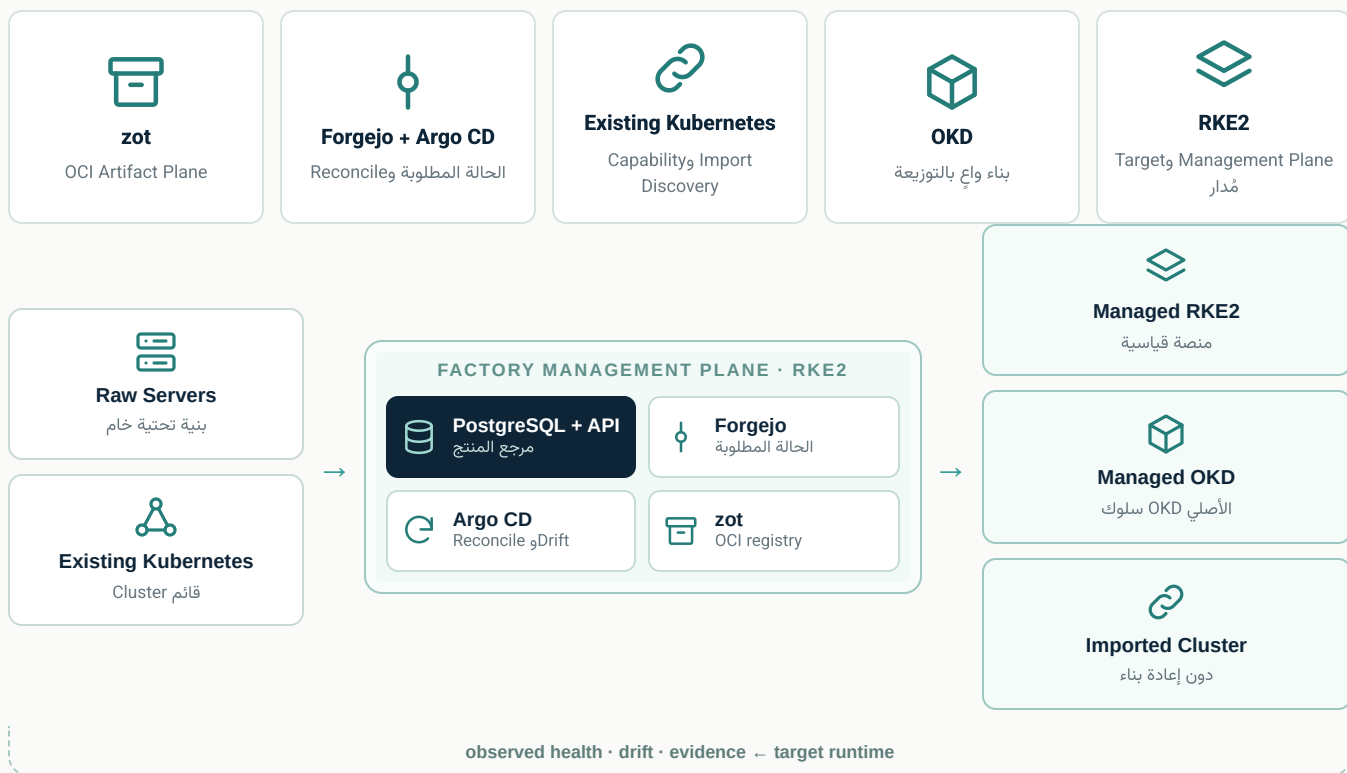


4SO Platform Factory

كتيب تقني

Build, Import and Operate Application Platforms

يحوّل الخوادم الخام أو Kubernetes القائم إلى منصات قياسية قابلة للإدارة؛ وتعمل
Product Control و Fleet و Release و Policy و Delivery والاستعادة تحت Plane واحد.



التوزيعة تبقى أصلية

لا يُختزل RKE2 و OKD إلى implementation اصطناعي واحد، ولا يُثبت Stack مكرر.

Authority منفصلة عن Runtime

Platform API و PostgreSQL هما مرجع المنتج؛ يحفظ Forgejo الحالة المطلوبة و Argo CD مجرد Reconciler.

لا يبني Factory ال Cluster فحسب؛ بل يحوّل Artifact و Capability و Distribution و Lifecycle إلى Platform Contract واحد.

CAPABILITY SNAPSHOT

Capability Snapshot

من البنية التحتية الخام إلى منصة التطبيقات

ليس مجرد أداة تثبيت؛ بل يغطي دورة Platform Engineering كاملة من إنشاء Target حتى تسليم Workload و Day-2 Operations.



GitOps

يحفظ Forgejo السجل ويحقق Argo CD التقارب



Fleet Operations

Maintenance و Drift و Health
لمجموعة Targets



Catalog & Blueprint

Template و Capability بإصدارات
للفرق



Create / Import

بناء Target مُدار أو ربط
Kubernetes قائم



Node & Upgrade

Drain و Replace و Upgrade واعية
بالتوزيع



Backup & Restore

Policy و Backup Run و Restore
Drill و



Workload Delivery

Application Release
Environment Binding و



Registry / Disconnected

zot وتسليم مستقل عن الإنترنت

المبادئ التشغيلية



تعمل Management Plane مستقلة على RKE2



لا تُثبت قدرات Target الأصلية مرة أخرى



ل Build plane و Target lifecycle مالكان منفصلان



نجاح الواجهة لا يحل محل أدلة Runtime

حدود ملكية المنتج



Product مرجع – PostgreSQL + Platform API
Authority



Forgejo – الحالة المطلوبة، لا Runtime truth



Argo CD – Reconciler، لا Source of Truth



zot – هوية كل Artifact و Provenance الخاص به

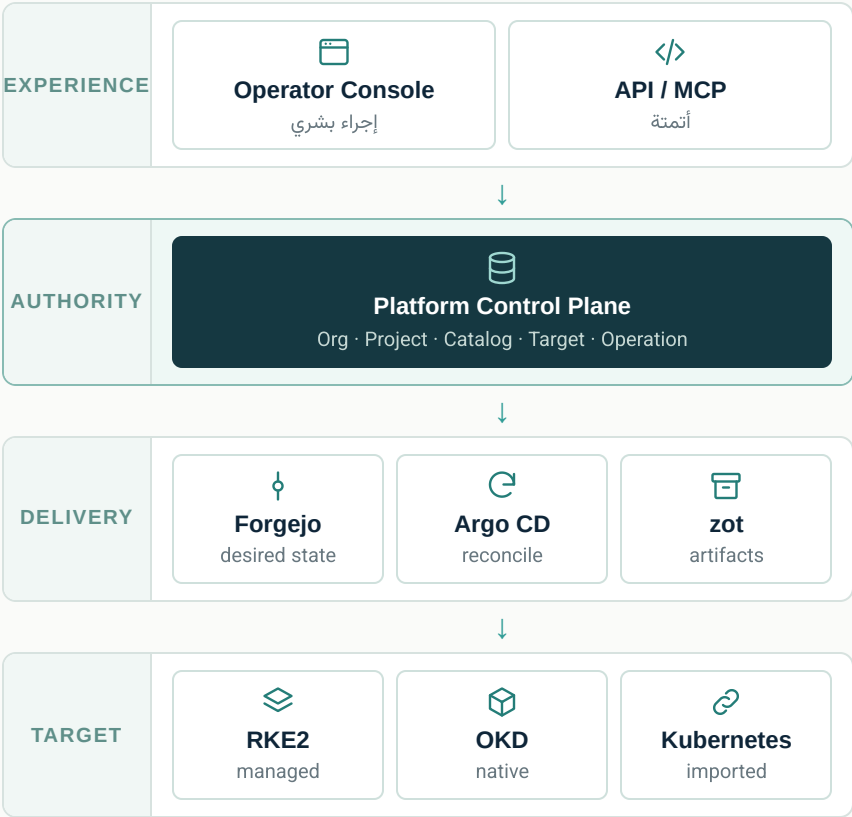
Core contract: Observed Target → Reconciliation → Desired State → Product Authority – لا يحل أي منها محل الآخر.



Architecture Overview

مرجع المنتج والحالة المطلوبة وبيئة التشغيل تبقى منفصلة

يحتفظ مرجع المنتج بالقرار ودورة الحياة، ويُسجّل تاريخ الحالة المطلوبة، ويطبّقها Reconciler، ويُظهر Target النتيجة.



- 01 Management Plane ≠ Target**
Target الإدارية ليست بحد ذاتها Target عامًا.
- 02 Artifact مرجع هو zot**
لا يحل Registry الداخلي في OKD محل zot.
- 03 Provider ≠ Distribution**
البنية التحتية المادية وهوية Distribution مفهومان منفصلان.
- 04 Trait مجرد Dapr**
اختياري ومن جهة Target؛ لا يستولي على authority المنتج.

المجال	Mechanism	السلوك
Managed OKD	openshift-install / oc + Redfish boot media	يُمر Provisioning على bare metal عبر عقد OKD نفسه.
Disconnected OKD	oc-mirror v2 → zot	تُختم Acquisition و Inventory و Mirror وتصبح قابلة للمراجعة قبل التثبيت.
Runtime trait	optional Dapr sidecar	Invocation و Pub/Sub و Binding؛ دون الاستيلاء على State أو Workflow أو Secret.

Targets & Platform Profiles

Factory واحد، وأنواع متعددة من Platform Target

تبقى Management Plane ثابتة؛ ويُعالَج اختلاف Distribution عند حدود Target لكي تتلقى كل بيئة ال Stack الذي تحتاجه فقط.

الاستخدام	Ownership	مسار الدخول	Target
self-contained و Private Cloud قياسية	دورة الحياة تحت Product Control Plane	بناء عبر Factory	Managed RKE2
إدخال Clusters قائمة تحت الإدارة	بيئة تشغيل قائمة + حدود دورة حياة المنتج	Discovery و Import	Existing Kubernetes
OpenShift-compatible منصة	OKD تملك قدراتها الأصلية	بناء وإع بالتوزيع	Managed OKD
إدارة دون تكرار الحزم الداخلية	OKD أصلية + إجراءات المنتج	Discovery و Import	Existing OKD



Imported Kubernetes
Identity discovery وقبول دورة الحياة

OKD Platform
واعية ب OVN و OLM و SCC؛ دون Stack مكرّر

RKE2 Platform
مُدارة · Fleet · Catalog add-ons

Fleet
العقد و Upgrade و Diagnostics والاستعادة

Disconnected
Install و Mirror و Acquire دون إنترنت

Application Platform
Binding وأدلة النشر و Release

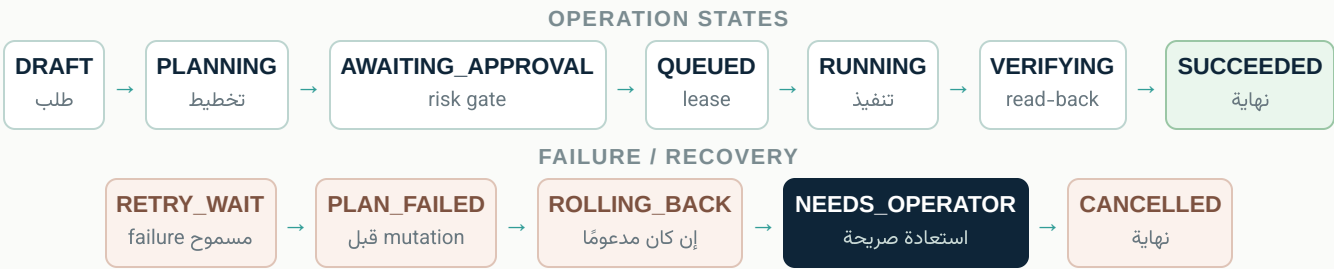
Topology-aware: لا تُكثّر القدرات الموجودة في Distribution؛ يحذف resolver الحزمة المكررة أو يجعلها اختيارية.

ACTION & WORKFLOW CONTRACT

Action & Workflow Contract

لكل Operation آلة حالات صريحة من Plan إلى Verification

verification و retry policy و approval و payload و risk و Operation class
المرصود جزء من نموذج المنتج.



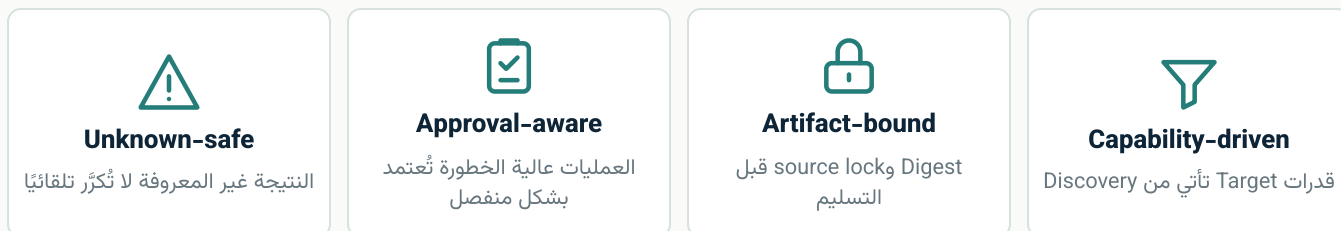
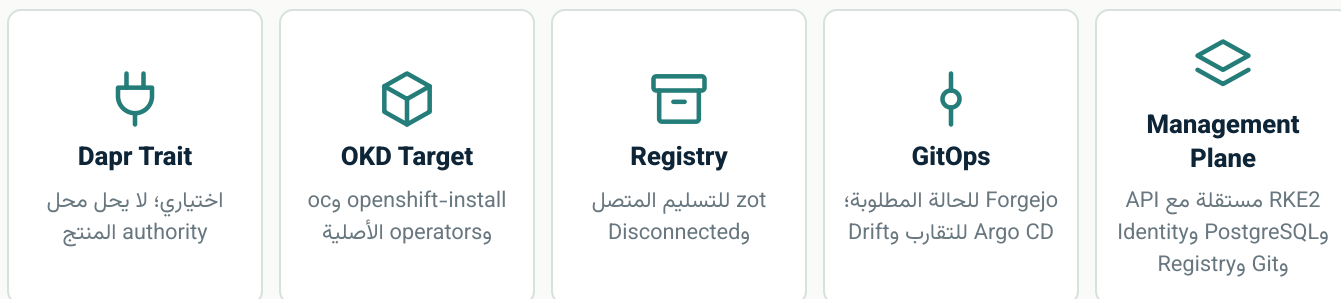
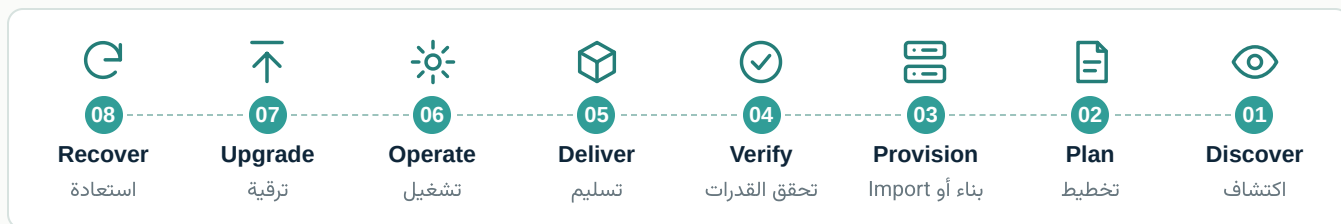
Failure / Recovery	Success	Execution / Lock	Admission	Action
PLAN_FAILED قبل التنفيذ؛ بعد side effect: retry / rollback / operator	Profile التقارب مع health و مرصود	+ payload مختوم exact-target fence	Profile ومدخلات Provider و Blueprint قابل للتخطيط	Create Platform
Import الناقص ليس Ready: conflict → operator	Target مسجل بقدرات مرصودة	دون إعادة بناء؛ register و classify	الوصول و identity و capability inventory	Import Cluster
نتيجة غير معروفة: recovery للقاء فقط، دون redispach	أدلة Deployment مطابقة لـ Binding	approval-gated target RBAC مع	Release غير قابل للتغيير + EnvironmentBinding	Deploy
RETRY_WAIT أو NEEDS_OPERATOR	العضو الجديد Ready والقديم drained	lease / fence ضد التنفيذ المتزامن	هوية العقدة و failure domain و safety admission	Node Replace
rollback فقط إذا دعمه workflow	health و version بعد كل مرحلة	مرحلي وواع بالتوزيعة	backup و compatibility و health أولي	Upgrade
mismatch → fail-closed	Artifact في zot inventory مطابق لـ	acquire → verify → mirror	inventory و source lock و digest	Disconnected

Retry محدود: لا يُعاد إلا failure classes المسموح بها؛ و rollback ليس وعدًا عامًا ويجب أن يدعمه workflow نفسه.

Lifecycle & Components

دورة حياة المنصة من Discover إلى Recover

لا يُبنى Target فحسب؛ فالإكتشاف والتخطيط والتحقق من القدرات والتسليم والتشغيل والترقية والاستعادة كلها جزء من دورة حياته.



☀️ **Day-2 First**: دورة حياة العقد و Upgrade و Backup و Restore و Diagnostics جزء من المنتج نفسه، لا ملحق به.

Recoverable 🔄

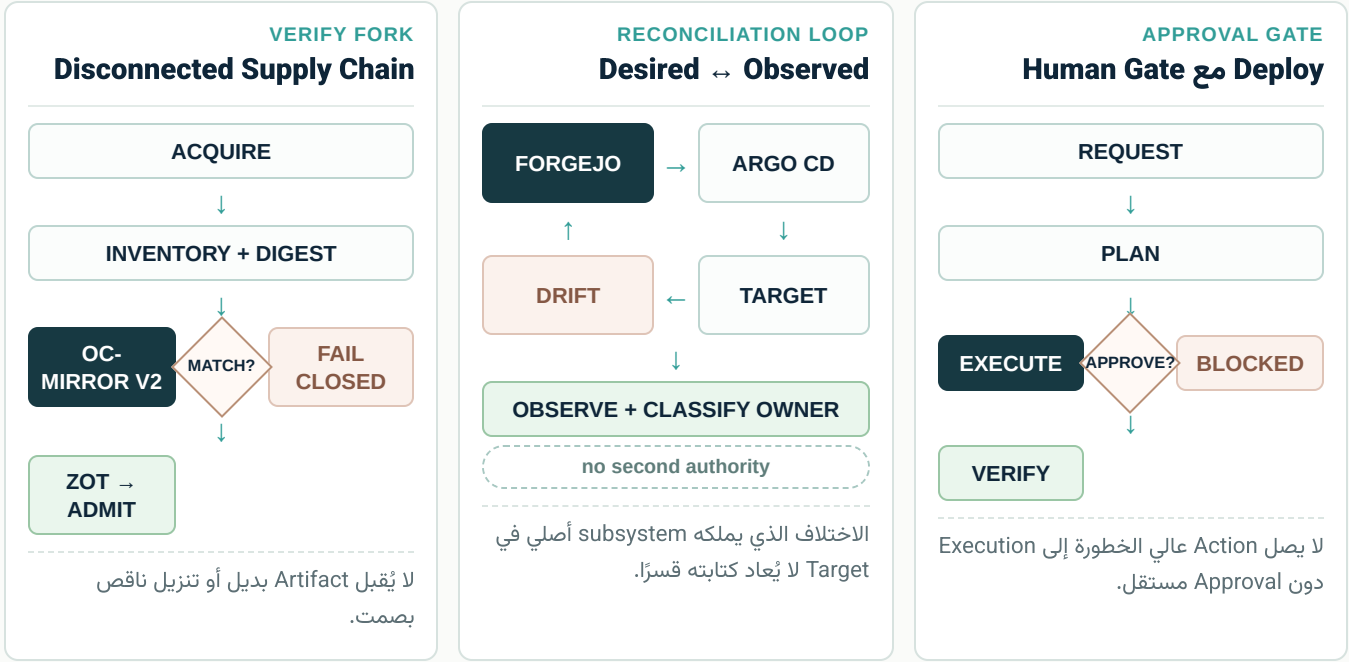
Operable ☀️

Observable 👁️

Standardized ✅

Failure & Recovery Semantics

ثلاثة مسارات غير خطية، لكل منها حد فشل واضح



Recovery	Product Behavior	Detection	Failure Domain
استعادة خدمات التحكم، ثم Reconcile	تستمر Workloads في Target قدر الإمكان	health وأدلة Operation	Management service
Reconcile للحالة المطلوبة	يُعلَم Drift؛ ولا تُعاد كتابة Authority	رصد Argo CD و Runtime	Target drift
الإصلاح والاستثناء من خطوة owner	لا يحدث تسجيل كاذب لـ Target	أدلة Provider و Installer	Provisioning
Seal و Acquire من جديد	يُحظر التسليم	مطابقة digest و inventory	Artifact mismatch
recovery للقراءة فقط أولاً	دون redispatch تلقائي	فقدان lease بعد side effect	Unknown outcome

Restore Drill: لا يُقبل Backup دون verification ولا Restore دون read-back على مستوى Workload كدليل على الاستعادة.

Action & Operations Catalog

عمليات على مستوى Intent، لا أوامر متفرقة



Fleet •

- remove
- drain
- add-node
- repair
- replace



Platform •

- status
- register
- import
- create
- diagnose



Delivery •

- deploy
- environment-bind
- release
- rollback-when-supported
- reconcile



Catalog •

- publish
- review
- revision
- revoke
- deprecate



Disconnected / OKD •

- oc-mirror-v2
- seal
- acquire
- upgrade-admit
- mirror-verify



Data Protection •

- backup-run
- backup-policy
- restore-run
- restore-drill

Observability والأدلة



الحالة المرصودة إلى جانب الحالة المطلوبة



Delivery Insights من أدلة النشر



Diagnostics محدودة دون كشف Secret

Identity والثقة



عضوية Org/Project و Service Account في مرجع المنتج



API token مع digest أحادي الاتجاه وصلاحيات محدودة



Credential الهدف بصيغة reference فقط

Action safety: لا يوجد target shell أو API proxy عام؛ لكل Action مالك ونطاق و risk و payload وعقد verification محدد.



تجاوزوا Cluster Management؛ واجعلوا Platform Engineering منتجًا.

يبنى 4SO Platform Factory منصات تبقى قياسية وقابلة للرصد والإدارة حتى بعد التسليم.

