

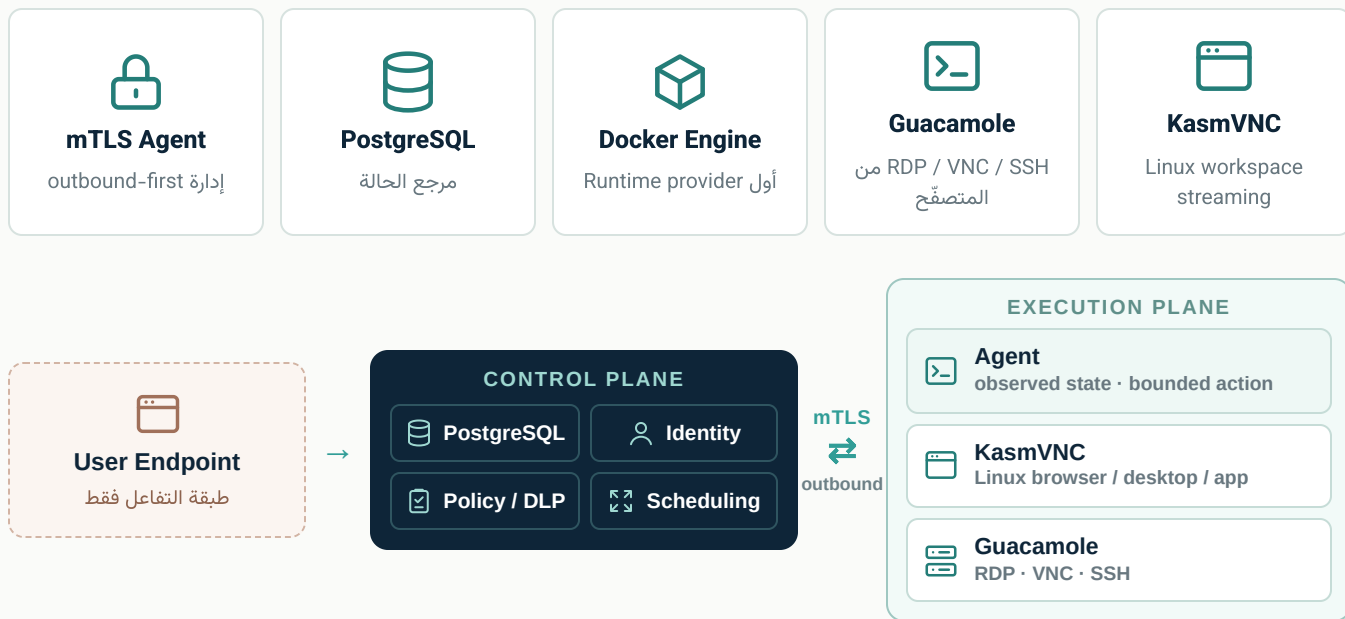
4SO Workspace

كتيب تقني

Secure Browser Workspaces with Separated Control & Execution Planes

RDP/VNC/SSH ووصول Linux و Desktop و Browser و Application على

من تجربة ويب واحدة؛ مع Identity و Policy و DLP و Scheduling ودورة حياة مستدامة ل Session، وتنفيذ محميّ منفصل عن جهاز المستخدم.



Single-node من الدرجة الأولى

يمكن أن يكون Control و Execution على Host واحد؛ Kubernetes خيار للنشر، وليس شرطاً للتجربة.

Endpoint ليس موضع الثقة

تبقى Session وتنفيذ workload داخل بيئة مضبوطة، ولا يمثّل Endpoint إلا طبقة التفاعل.

افصلوا بيئة العمل عن Endpoint؛ وأبقوا تجربة المستخدم بسيطة.



CAPABILITY SNAPSHOT

Capability Snapshot

تجربة مستخدم بسيطة، وبنية تحتية جادة خلفها

يجمع Workspace قدرات User Experience و Infrastructure Operations جنباً إلى جنب في منتج واحد.



Policy و DLP

Peripheral و Clipboard و File
Network Path و



الهوية المؤسسية

Authorization و Authentication
والنطاق



RDP / VNC / SSH

وصول من المتصفح دون عملاء
متفرقين



App و Desktop و Browser

بيئات Linux مؤقتة ومضبوطة



Observability

Audit و Capacity و Health
في رؤية واحدة



Recording

مراقبة وتعاون Audit على مستوى
Session



Multi-zone

توسيع Execution دون نقل
Control



Capacity و Scheduling

اختيار عقدة التنفيذ بناءً على الحالة

مبادئ التشغيل



إدارة العقد outbound-first وعبر mTLS



لا تمرّ Browser UI إلا عبر Product API



تُرصّد حالة Session من Runtime



Kubernetes اختياري، وليس شرطاً مسبقاً

حدود ملكية المنتج



PostgreSQL – Intent
Capacity و Session و Policy و Node



Control ≠ Execution – دوران مستقلان



Agent – حالة مرصودة، لا Authority



Single-node – نموذج نشر من الدرجة الأولى

Core contract: Session = Intent + Durable Operation + Runtime Observation – لا تُعدّ أي مرحلة بمفردها

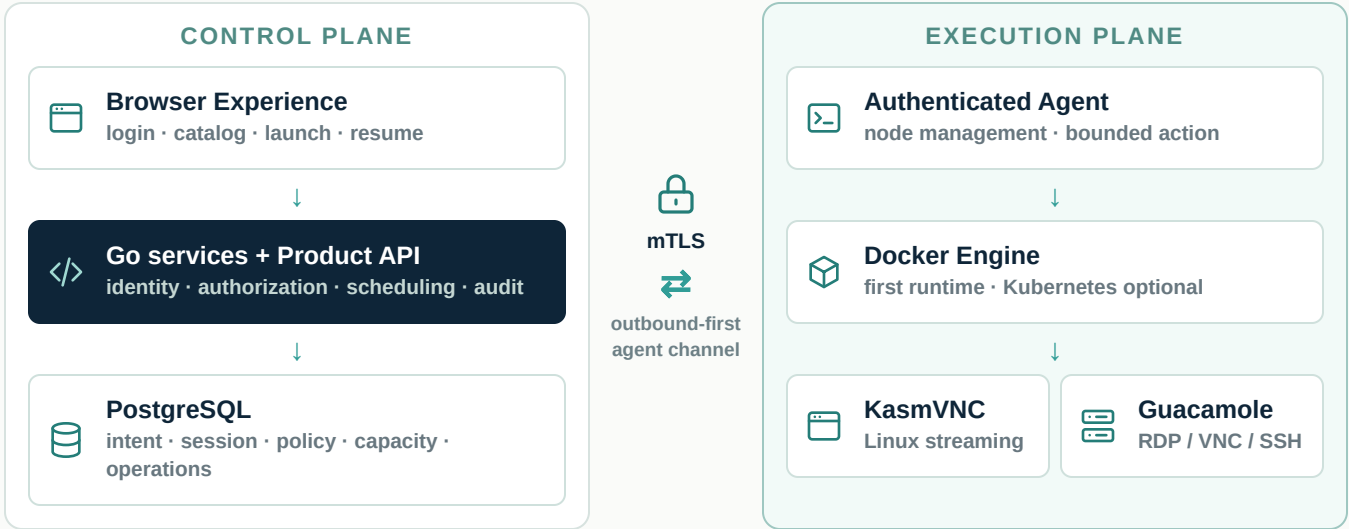
نجاحاً.



Architecture Overview

Execution Plane و Control Plane ليسا شيئاً واحداً، عن قصد

يبقى Policy و Intent في Control Plane؛ وتتولّى الوكلاء (Agents) الإدارة، بينما تعمل Session الفعلية في Execution Plane.



الطبقة	Component	العقد
State Authority	PostgreSQL	لا تُنشئ UI ولا Agent مصدراً مستقلاً للحالة
Control Plane	Go services + Product API	Execution و Identity و Scheduling و audit؛ بمعزل عن Execution
Agent Plane	Outbound-first mTLS agents	تمرّ Authority عبر Product API و RBAC
Linux Streaming	KasmVNC	يبقى التنفيذ المحميّ على Execution Plane
Remote Access	Apache Guacamole	البروتوكول البعيد خلف Identity و Policy نفسيهما



Observed, not assumed
نُقرأ حالة Session من Runtime



No direct mutation
لا تُجري UI تغييراً مباشراً على Runtime



Deterministic release
تُسَلَّم API و Controller و Edge و CLI و migrations في artifact واحد

Deployment & Install Contract

من خادم واحد إلى Execution Plane متعدد المناطق

الاستخدام	Execution	Control Plane	الملف التعريفي
بداية بسيطة وبيئة صغيرة	الخادم نفسه	الخادم نفسه	عقدة واحدة
فصل الإدارة عن تنفيذ Workspace	عدة عُقد تنفيذ	مستقل	Control + عُقد التنفيذ
القرب من المستخدم وتوزيع السعة	Execution في عدة Zones	مركزي	Multi-zone
تكرار Control Plane	Execution Pool مستقل	متعدد العُقد	HA Control Plane

ARTIFACT-BOUND INSTALL



Safe resume

resume_required

owner من last_safe_resume_point و boundary

Unsafe cache rejected

ثُرفض Hard-link و permission غير الآمنة

Loopback TLS edge

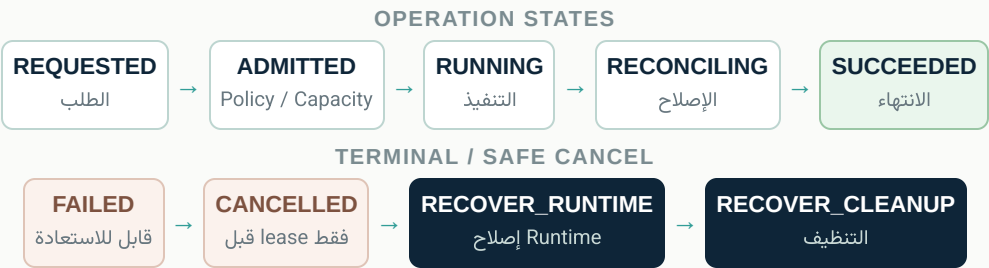
لا يُنشر PostgreSQL و Control API على Host

Workspace لا تعتمد تجربة Product lifecycle؛ No Kubernetes tax: Runtime provider تفصيل تنفيذي تحت Product lifecycle؛ ولا تعتمد تجربة Workspace العادية على Kubernetes.

Action & Workflow Contract

Session ليست طلباً لحظياً

تنتقل Launch وStop وRestart وRecovery من Product API إلى Operation
وOutbox، وتُرصّد حالة Session بمعزل عن حالة الطلب.



Failure / Recovery	Success	Execution / Lock	Admission	Action
retry أو recovery event؛ لا تخمّن UI النتيجة	Session ID وRuntime مرصود	Idempotency-Key → Operation / Outbox → Scheduler / Agent	صلاحية Actor/Project وPolicy وCatalog وCapacity	Launch
قابلة للإلغاء قبل lease؛ وبعده Reconcile	لم تعد Session في حالة running	Operation مستقلة إلى Agent / Runtime	Session قائمة وصلاحية سارية	Stop
يُحفظ Correlation بين المصدر والخلف	Successor مرصودة وقابلة للاستخدام	Restart attempt + successor binding	Source session صالحة	Restart
عدد المحاولات وتوقيتها في History	Runtime في حالة Ready مجدداً	RECOVER_RUNTIME صريح، لا restart عام	حالة failure / recovery	Recover Runtime
دون إعلان نجاح زائف لخلف	موارد يتيمة مُنظّفة ومتقاربة	RECOVER_CLEANUP على Session نفسها	Runtime غير مكتمل يمكن إثباته	Recover Cleanup
لا تُترك Session نشطة يتيمة بصمت	Placement من الحالة المرصودة	Scheduling منسّق مع دورة حياة العقدة	Health والسعة قبل / Add Drain / Remove	Node Capacity

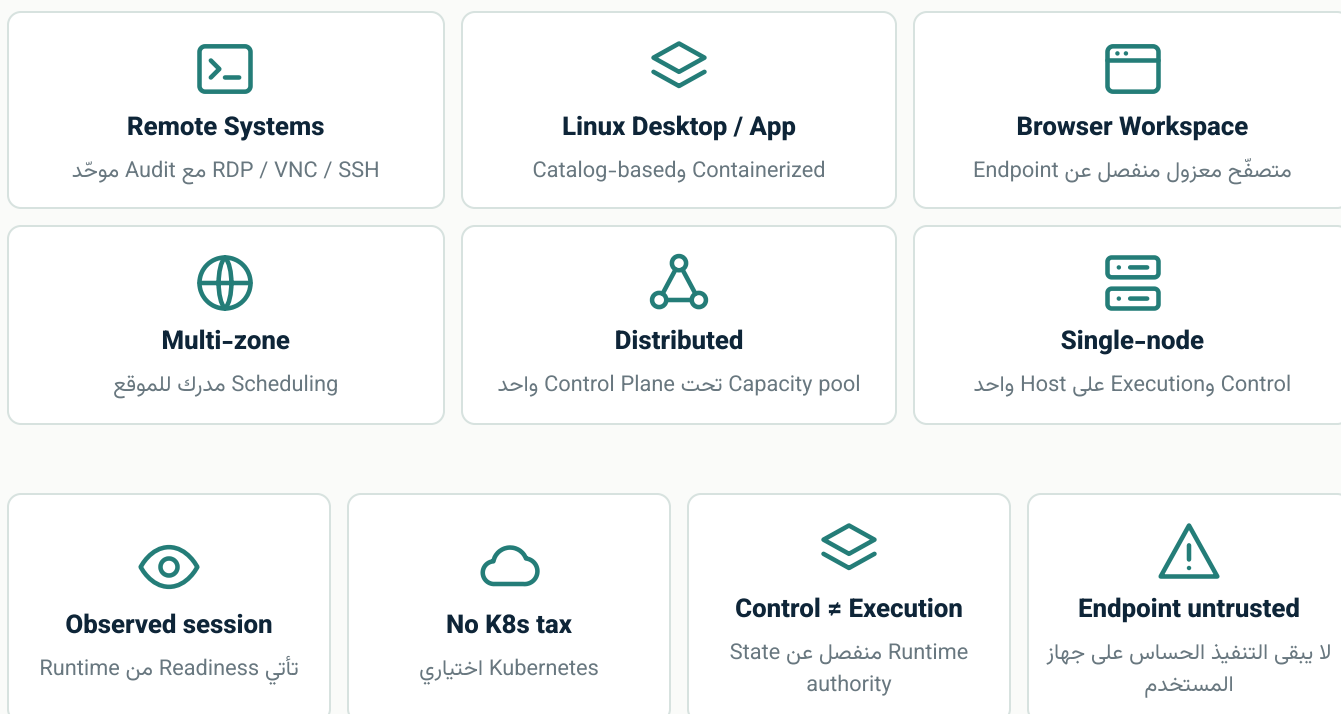
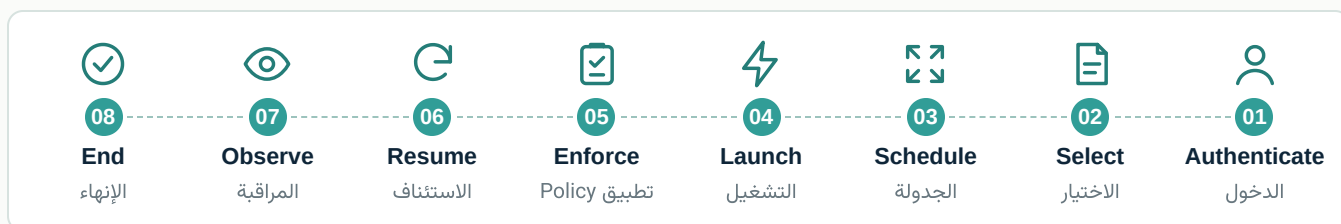
Safe cancel: فقط في REQUESTED أو ADMITTED، دون lease owner وقبل عبور حدّ side effect؛ ويحتفظ History بالمحاولات وآخر recovery.



Lifecycle & Workspace Profiles

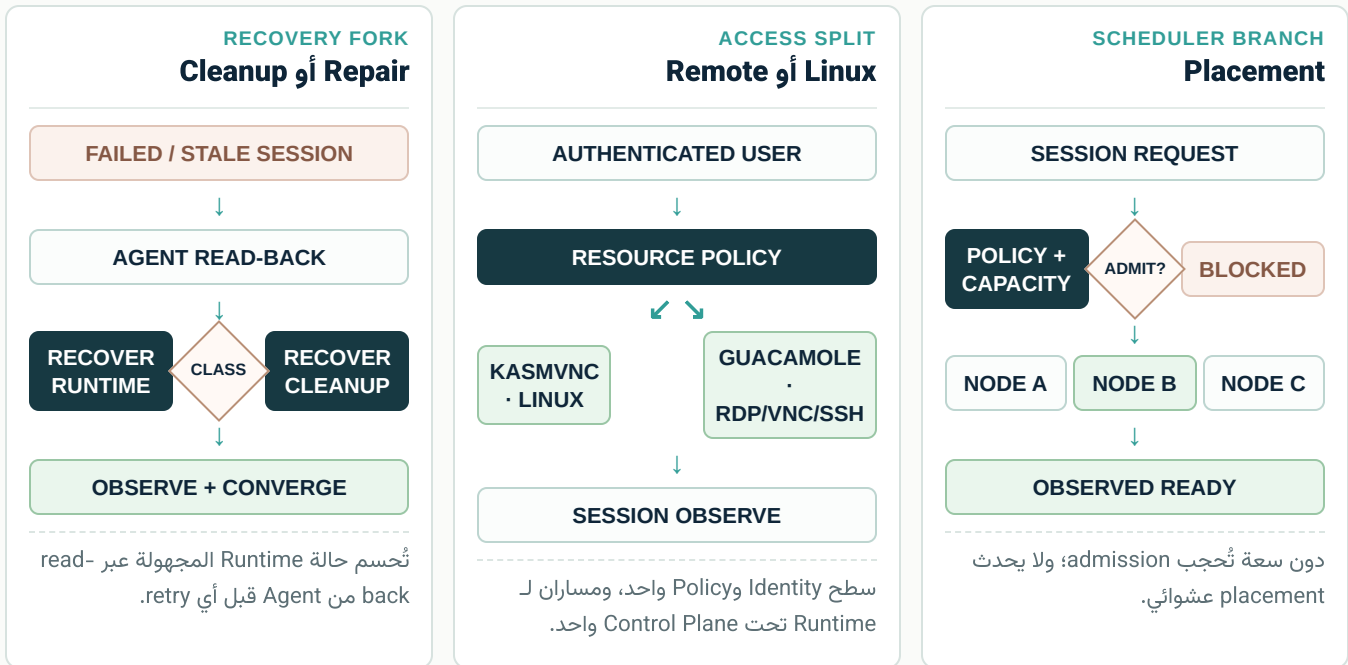
Session ليست مجرد Launch

من المصادقة إلى Scheduling وتطبيق Policy و Resume و Recording والإنهاء، كل ذلك جزء من دورة حياة المستخدم والمستخدم والبنية التحتية.



Failure & Recovery Semantics

لكل من Browser و Control و Agent و Runtime أعطال مختلفة



Recovery / Fence	Product Behavior	Detection	Failure Domain
Reattach دون إعادة بناء Authority	يمكن أن يستمر Runtime	Session و Telemetry العميل	Browser disconnect
إعادة اتصال Agent و Reconcile	Mutation جديدة محجوبة أو degraded	Heartbeat والحالة المرصودة	Agent unavailable
Restart أو RECOVER_RUNTIME	Session تحتاج إلى انتباه أو استعادة	حالة failure في Session	Runtime crash
RECOVER_CLEANUP	لا يُعلن نجاح جديد	اكتشاف موارد يتيمة	Partial cleanup
Policy و Relaunch و Drain وفق Policy	تتغير Admission	حالة Scheduler والعقدة	Capacity loss

Data protection: Session المؤقتة ليست بيانات المستخدم الدائمة؛ ولا ينبغي لاستبدال العقدة أن يترك هوية Session دون Reconcile.



Action & Operations Catalog

Infrastructure Journey و User Journey في منتج واحد



Session •

recover-runtime

restart

stop

recover-cleanup



Workspace •

status

launch

catalog-list

attach



Capacity •

rebalance

schedule

observe



Node •

remove

drain

preflight

register

replace



Diagnostics •

operation history

status-json

doctor



Policy •

access scope

network policy

DLP

Evidence و Observability |



Session و Status و attention ومحاولات recovery في Session



حالة العقدة و Capacity للمشغل



Unknown بدلاً من Healthy مُحَمَّن

Trust و Identity |



Identity و RBAC قبل admission



mTLS لاتصال Agent وثقة العقدة



Credential لمرة واحدة؛ دون Secret في JSON

Action safety: تستهلك UI و Agent واجهة Product API نفسها؛ ولا مكان ل shell أو runtime bypass في workflow العادي.

Workspace آمن، دون تحويل Endpoint إلى حدّ الثقة.

يحوّل 4SO Workspace الوصول الآمن من اتصالات متفرقة إلى منتج واحد قابل للإدارة.

4SOLab · 4SO Workspace