BareStax

No layers. Just compute.

النظرة العامة التقنية لـ BareStax

البنية ودورة الحياة والتشغيل والأمن والتثبيت والترخيص لعناقيد NVIDIA GPU داخل مراكز بيانات المؤسسة

الإصدار 2026-11 · barestax.io

المحتويات

01 البنية المعمارية ودورة حياة العنقود في نظام واحد

02 قدرات هندسية تغطي كل طبقة من العتاد حتى طابور المهام

03 واجهة تشغيل واحدة للمشغّلين والباحثين دون اعتماد على الإنترنت

04 الأمن جزء من آلية التشغيل نفسها لا طبقة مضافة لاحقاً

05 متطلبات واضحة ومسار تثبيت موحّد للشبكات المتصلة والمعزولة

06 ترخيص بسيط لبنية تحتية سيادية

07 صُمّم للمؤسسات التي تملك وحدات GPU الخاصة بها

08 إجابات تقنية واضحة حول بنية BareStax وتشغيله

01

البنية المعمارية ودورة حياة العنقود في نظام واحد

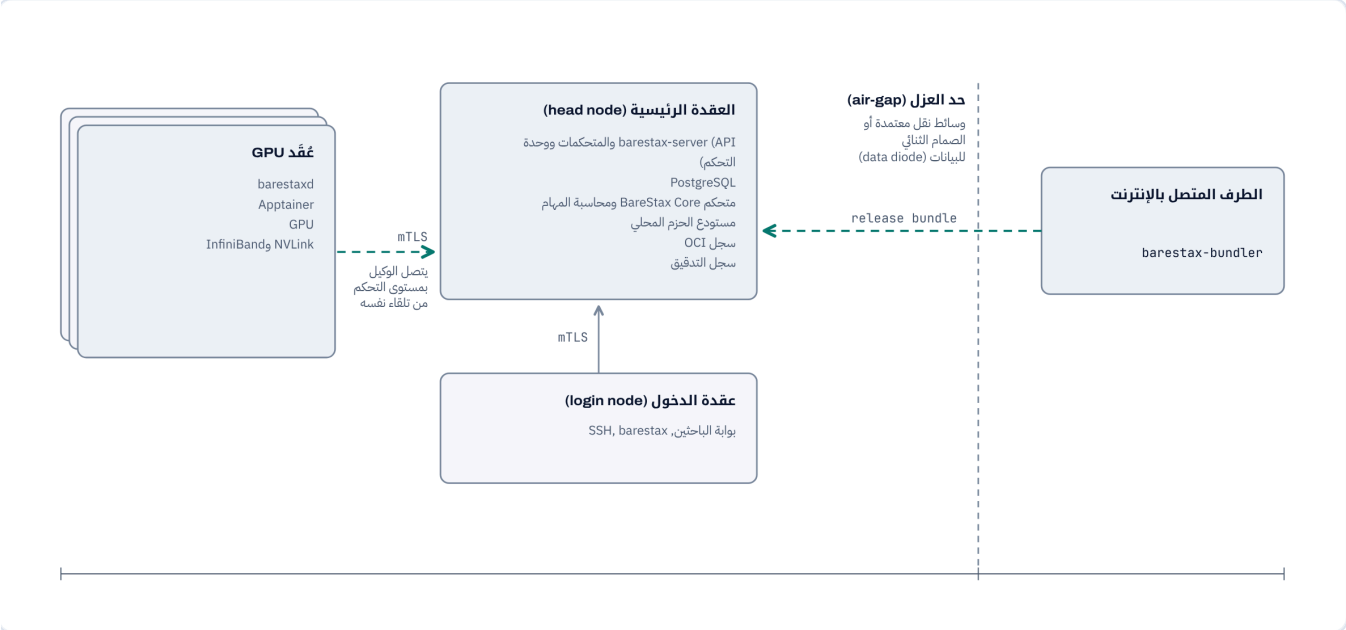
يدير BareStax دورة حياة عنقود NVIDIA GPU كاملة عبر مستوى تحكم مركزي ووكيل يعمل على كل عقدة حساب وجدولة BareStax Core مدمجة. يستغني هذا التصميم عن طبقات المحاكاة الافتراضية ومنصات تنسيق الحاويات الوسيطة، فيمنح المهام وصولاً مباشراً إلى العتاد والشبكة.

أربعة مكوّنات مترابطة عبر اتصال mTLS متبادل

تتكوّن بنية BareStax من أربعة أجزاء واضحة الحدود. ويُوزَّع البرنامج كملفات تنفيذية مستقلة مكتوبة بلغة Go: `barestax-server` و `barestaxd` و `barestaxctl` و `barestax` و `barestax-bundler` . وتأتي وحدة التحكم الرسومية مدمجة داخل `barestax-server` :

- **العقدة الرئيسية (head node):** تشغّل `barestax-server` (الواجهة البرمجية والمتحكمات ووحدة التحكم الرسومية) وPostgreSQL ومتحكم BareStax Core ومحاسبة المهام ومستودع الحزم المحلي وسجل صور OCI وسجل التدقيق. تعمل على خادم فيزيائي دون معالجات GPU أو داخل آلة افتراضية على منصة المحاكاة المعتمدة لدى المؤسسة.
- **عُقَد GPU:** تشغّل وكيل العقدة `barestaxd` المسؤول عن الانضمام وجرد العتاد والتثبيت عبر وحدات (modules) ومسابير الصحة، إلى جانب Apptainer. يبادر الوكيل بالاتصال بمستوى التحكم من تلقاء نفسه، ولا تُرسَل أوامر من الخارج إلى العُقَد.
- **عقدة الدخول (login node):** تمثّل نقطة دخول الباحثين عبر SSH وبوابة الباحثين لإرسال المهام إلى BareStax Core ومتابعتها.
- **الطرف المتصل بالإنترنت:** يشغّل أداة `barestax-bundler` التي تجمّع حزم الإصدار وتوقّعها قبل نقلها عبر وسائط معتمدة أو الصمام الثنائي للبيانات (data diode) إلى البيئة المعزولة عن الإنترنت (air-gap).

تتم جميع الاتصالات الداخلية عبر mTLS بالاعتماد على بنية PKI الخاصة بالعنقود مع تجديد الشهادات.



المخطط المعماري لنظام BareStax يوضح الطرف المتصل بالإنترنت وحد العزل والعقدة الرئيسية وعُقَد GPU وعقدة الدخول واتصالات mTLS.

تأسيس مستوى التحكم في اليوم 0 واختبار التنبيهات

يبدأ تأسيس العنقود بتشغيل أمر تهيئة واحد على العقدة الرئيسية مع حفظ نسخة احتياطية لمفاتيح العنقود في الملف المحدد. يعرّف المشغّل بعد ذلك مصادر الهوية (LDAP وActive Directory والحسابات المحلية وOIDC وSAML) والعامل الثاني المدمج TOTP وإعدادات الشبكة وأهداف التخزين المشترك NFS وS3.

ويُختتَم اليوم 0 باختبار عملي لمسار التنبيهات يصل إلى المناوب ويُؤكَّد برمز التحقق قبل إدخال أول عقدة حساب.

```
barestax-server init --cluster-name <name> --endpoint <fqdn> --key-backup <file>
barestaxctl alert test
```

انضمام العقدة في اليوم 1 والتحقق المسبق من العتاد

قبل انضمام الخادم العامل بنظام Ubuntu 24.04 LTS إلى العنقود، يفحص النظام الحد الأدنى لإصدار البرمجيات الثابتة (firmware) وحالة الأقراص وإعداد Secure Boot وسلامة الاتصال. وبعد تنفيذ أمر الانضمام واعتماد العقدة بموافقة واحدة، يجرد الوكيل بنية GPU وNVLink وInfiniBand وPCIe وNUMA ويطابق الخادم مع ملف التعريف المناسب.

يثبّت النظام من المستودع المحلي مجموعة متوافقة جرى اختبارها معاً تضم النواة المثبّتة وDOCA-OFED وتعريف NVIDIA ومكتبات CUDA وFabric Manager وDCGM وNCCL وApptainer. تخضع العقدة عقب التثبيت لاختبارات GPU وNVLink وInfiniBand واختبار NCCL بين عقدتين، ولا تدخل طابور BareStax Core لاستقبال المهام إلا بعد اجتيازها بالكامل.



مخطط تدفق انضمام العقدة من التركيب في الرف وتنفيذ أمر واحد والموافقة حتى تثبيت المكدس والتحقق والجهوزية في BareStax Core.

التشغيل المستمر في اليوم 2 وتصحيح الانحراف والاسترداد

يراقب النظام حالة كل عقدة باستمرار لرصد أي انحراف (drift)؛ فيصحّح الانحراف الذي لا يتطلّب توقفاً تلقائياً أثناء بقاء العقدة في الخدمة، أمّا الانحراف الذي يستلزم توقفاً كاختلاف النواة فلا يمسّه من تلقاء نفسه بل يبلّغ عنه بانتظار تطبيقه في نافذة الصيانة. وتُقيَّم الإشارات الصحية لمعالجات GPU والروابط الشبكية والذاكرة والتخزين في الوقت الفعلي؛ فإذا تعثرت عقدة، يتوقف إسناد المهام الجديدة إليها ريثما تكتمل مهامها النشطة مع حماية ضد التذبذب المتكرر.

يسير الاسترداد المتدرج من إعادة تشغيل الخدمة إلى إعادة إقلاع النظام ثم دورة الطاقة عبر BMC، وتحدد السياسة أي خطوات تعمل تلقائياً وأيها يتطلّب اعتماداً بينما تُنفَّذ عمليات طاقة BMC كعمليات معتمدة فقط. ويوقف مكبح العواصف سلسلة الاسترداد تلقائياً عند حدوث عطل جماعي يصيب عدة عُقَد في آن واحد، فيما يكشف عرض الأثر المهام والمستأجرين والخدمات المتأثرة.



مقارنة جنباً إلى جنب بين الحالة المطلوبة في ملف التعريف والحالة المرصودة على العقدة حيث يُصحَّح السطر المختلف دون مقاطعة المهام الجارية.

الترقيات المرحلية وإخراج العُقَد بأمان

تُطبَّق التحديثات باستخدام حزم إصدار موقّعة وفق أسلوب النشر المرحلي: تُرقّى عقدة واحدة أولاً للتحقق من سلامة التشغيل، ثم تتبعها بقية العُقَد بعدد متزامن لا يتجاوز ميزانية التوقف المحددة مع الحفاظ على المهام الجارية، ويُرقّى مستوى التحكم بالمسار ذاته.

عند الحاجة إلى صيانة عتاد أو استبداله، يفرّغ أمر واحد العقدة من المهام ويزيلها من العنقود دون فقدان أي عمل قيد التنفيذ، وتُبطَل شهادة هويتها السابقة فوراً مع السماح بإعادة ضمّها لاحقاً بالاسم ذاته.

```
barestaxctl node drain gpu-07
barestaxctl node remove gpu-07
```

واجهة برمجية تصريحية توحّد وحدة التحكم وسطر الأوامر

يعتمد BareStax نموذج موارد تصريحياً يفصل بين الحالة المطلوبة (spec) والحالة الفعلية التي يكتبها الخادم (status) مع تدفق متابعة حي للتغييرات. يتيح وضع المعاينة (plan وdry-run) فحص أثر أي تعديل قبل تطبيقه، وتستدعي وحدة التحكم الرسومية وأداة `barestaxctl` الواجهة البرمجية نفسها دون استثناء.

```
barestaxctl plan -f <file>
barestaxctl apply -f <file>
```

استمرارية المهام عند غياب مستوى التحكم واستعادة نظيفة

لا تتأثر المهام الجارية على عُقَد الحساب في حال انقطاع مستوى التحكم أو توقفه، إذ تحتفظ العُقَد بآخر حالة آمنة معروفة وتمنع بوابة الصحة المحلية إسناد مهام إلى أي عقدة متعطلة. وتشمل النسخة الاحتياطية لمستوى التحكم كلاً من الهوية وبنية PKI وقاعدة البيانات وحالة BareStax Core، مع استعادتها على عتاد نظيف وعزل العقدة الرئيسية القديمة لمنعها من الاستجابة بعد الاستعادة.

02

قدرات هندسية تغطي كل طبقة من العتاد حتى طابور المهام

يدير BareStax المكوّنات اللازمة لحوسبة GPU عالية الكثافة ضمن نظام تشغيلي واحد بدلاً من نصوص وأدوات منفصلة. تمتد الإدارة التصريحية من النواة والتعريفات والنسيج الشبكي حتى جدولة BareStax Core وسلسلة الثقة بالصور وحزم الإصدار المعزولة عن الإنترنت.

إدارة المكدس التصريحي

- **ملفات تعريف شاملة للعقدة:** تُوصَف الحالة المستهدفة لكل عقدة في ملف تعريف يحدّد إصدار النواة ومكدس الشبكة DOCA-OFED وتعريف NVIDIA ومكتبات المستخدم CUDA وFabric Manager وDCGM وNCCL وApptainer إلى جانب معاملات sysctl واسم المضيف ومزامنة الوقت.
- **مجموعات متوافقة وتثبيت النواة:** لا تُنشَر المكوّنات إلا في مجموعات جرى التحقق من توافقها معاً، وتُثبَّت النواة عند الإصدار المعتمد بحيث لا تتمكّن التحديثات التلقائية لنظام التشغيل من كسر التوافق مع التعريفات أو الشبكة.
- **رصد الانحراف والتعامل مع نوعيه:** يكشف النظام أي تعديل يدوي أو تغيّر غير متوقع في العقدة؛ فيُصحَّح الانحراف الذي لا يستلزم توقفاً والعقدة في الخدمة، بينما يُبلَّغ فقط عن الانحراف الذي يتطلّب توقفاً دون تغيير أي شيء حتى يُطبَّق بعملية معتمدة خلال نافذة الصيانة.
- **فحوص ما قبل الانضمام:** يتحقق النظام قبل انضمام العقدة من الحد الأدنى لإصدار البرمجيات الثابتة وسعة الأقراص وحالة Secure Boot وسلامة الاتصالات الشبكية.
- **اكتشاف العتاد ومطابقة ملف التعريف:** يجرد النظام عقب اعتماد الانضمام معالجات GPU وروابط NVLink وبطاقات InfiniBand ومسارات PCIe وتوزيع NUMA، ويسجّلها في الجرد ليربط العقدة بملف التعريف المطابق لعتادها.

جدولة BareStax Core وتشغيل أحمال العمل

- **إعداد BareStax Core مركزي ومحاسبة مدمجة:** يولّد النظام إعدادات BareStax Core ويوزّعها مركزياً على جميع العُقَد، وتأتي خدمة محاسبة المهام مهيّأة وجاهزة منذ التأسيس.
- **طوابير متعددة المستأجرين وفئات العتاد:** يدعم النظام طوابير مصنّفة حسب فئة GPU وطوابير مخصّصة لمعالجات CPU، مع تقسيم المستأجرين وتحديد الحصص وتطبيق سياسة fairshare.
- **تخصيص متوازن للموارد وعرض النطاق:** تُحجَز حصة أنوية CPU تلقائياً مقابل كل معالج GPU مخصّص للمهمة، بما يمكّن مهام التدريب الموزّعة متعددة العُقَد من بلوغ عرض النطاق الحقيقي للنسيج الشبكي.
- **ثلاثة مسارات لإرسال المهام:** يرسل المستخدمون أعمالهم مباشرة من سطر الأوامر، أو عبر قوالب `barestax run` الجاهزة للمهام الدفعية ومصفوفات المهام وتدريب torchrun متعدد العُقَد والجلسات التفاعلية، أو عبر نموذج الويب في بوابة الباحثين.
- **المهام القابلة للإزاحة وإعادة الجدولة والخدمات طويلة الأمد:** يدعم النظام المهام القابلة للإزاحة (preemptible)، ويعيد إدراج المهام المُرسَلة عبر قوالب `barestax run` في الطابور بأمان عند تعطل عقدة، كما يوفّر طوابير مستقلة للخدمات طويلة الأمد مثل خوادم النماذج مع تسجيل الخدمة وحمايتها وإتاحة الوصول الخارجي عبر موازن الحمل الخاص بالمؤسسة.
- **شفافية الطوابير والحصص:** يرى كل باحث حصته والسبب الفعلي لانتظار مهمته في الطابور.

حاويات Apptainer وسلسلة الثقة بالصور

- **تشغيل عبر Apptainer دون Docker:** تنفَّذ جميع أحمال العمل داخل حاويات Apptainer، ولا يُستخدم Docker على عُقَد الحساب.
- **سجل OCI مدمج ومسار ترقية خاضع للرقابة:** يتضمّن مستوى التحكم سجل صور OCI يستورد الصورة ويفحصها أمنياً، ثم لا ترقّى للاستخدام إلا بموافقة شخصين (أربع أعين) وتوقيعها بمفتاح العنقود.
- **منع الصور غير الموقّعة على عُقَد الحساب:** ترفض عُقَد الحساب بدء أي حاوية لا تحمل توقيعاً معتمداً، مع دعم الربط بسجل المؤسسة الخاص واعتماد التوقيع المقابل للمؤسسة.
- **ثبات البيئة وفصل التخزين المؤقت:** تبقى صورة الحاوية للقراءة فقط أثناء التنفيذ، بينما تُحفَظ حزم المستخدم وذاكرة النماذج المؤقتة داخل مساحة عمله الدائمة.

مراقبة الصحة والتشخيص والاسترداد المتدرج

- **إشارات صحية شاملة للعتاد والخدمات:** يراقب النظام أخطاء GPU (بما فيها XID وECC وإعادة تعيين الصفوف وتقييد الحرارة والطاقة) وروابط NVLink وNVSwitch وشبكات InfiniBand وRoCE وأخطاء PCIe (AER) والذاكرة (EDAC) وجودة تزامن الساعة والخدمات الحرجة واتصال التخزين المشترك.
- **الوضوح عند تقادم القياسات:** إذا تأخّر ورود القياسات وتجاوزت صلاحيتها الزمنية، يصنّف النظام حالة العنصر كغير معروفة ولا يعرض بيانات قديمة كما لو كانت حيّة.
- **تفريغ انتقائي وعزل يدوي وحماية من التذبذب:** تتوقف العقدة المتعطلة عن قبول مهام جديدة (drain) ريثما تنتهي المهام الجارية عليها مع حماية من التذبذب تمنع التفريغ غير المبرّر، كما يستطيع المشغّل عزل عقدة يدوياً (Cordon) لإيقاف المهام الجديدة عنها أثناء الصيانة أو التشخيص مع استمرار مهامها الجارية.
- **استرداد متدرج ومكبح للعواصف:** يطبّق النظام خطوات استرداد متدرجة تشمل إعادة تشغيل الخدمة ثم إعادة إقلاع نظام التشغيل ثم دورة الطاقة، وتحدد السياسة ما يعمل منها تلقائياً وما يتطلّب اعتماداً، بينما يوقف مكبح العواصف سلسلة الاسترداد عند الأعطال الجماعية لحماية العنقود من إيذاء نفسه.
- **ميزانية التوقف وعرض الأثر:** يحدّد المشغّل العدد الأقصى للعُقَد المسموح بخروجها من الخدمة في آن واحد ونوافذ الصيانة، ويعرض النظام أثر كل عطل أو هدف تخزين أو تنبيه على المهام والمستأجرين والخدمات مع بيان عمر البيانات والفصل بين الأثر المؤكد والمحتمل.
- **تشخيص عميق وبوابة صحة محلية:** ينفّذ أمر واحد تشخيصاً عميقاً لمعالجات GPU على العقدة، وتواصل بوابات الصحة المحلية على العُقَد منع إسناد المهام للعقدة المتعطلة حتى لو غاب مستوى التحكم.

التشغيل المعزول عن الإنترنت وحزم الإصدار

- **استقلالية تامة عن الإنترنت:** لا يحتاج أي مسار تشغيلي في BareStax إلى اتصال بالإنترنت أثناء التأسيس أو التشغيل اليومي أو الترقية.
- **تجميع وتوقيع حزم الإصدار:** يجمع `barestax-bundler` على الطرف المتصل جميع المكوّنات اللازمة في حزمة إصدار موقّعة ومفهرسة بالمحتوى، وتُنقل عبر وسائط نقل معتمدة أو الصمام الثنائي للبيانات (data diode).
- **فحص واعتماد مزدوج عند الاستيراد:** يتحقق النظام عند استيراد الحزمة من صحة التوقيع وسلامة المحتوى والتوافق مع العنقود ويرفق تقرير الفحص، ولا تُعتمد للنشر إلا بموافقة شخصين.
- **تثبيت المستودعات ومراسم المفاتيح:** تُثبَّت المستودعات المصدرية بلقطات زمنية محددة وتُحفَظ بصمات مفاتيحها داخل قسم الثقة في الحزمة لإنتاج البايتات ذاتها في كل تثبيت، بينما تُولَّد مفاتيح توقيع الإصدارات في بيئة غير متصلة بالشبكة ضمن مراسم مفاتيح مسجّلة، وتثبّت العُقَد حزمها من المستودع المحلي للعنقود.

الأمن والهوية وسجل التدقيق

- **اتصال mTLS وبنية PKI داخلية:** تجري كل الاتصالات داخل العنقود عبر mTLS بشهادات يصدرها العنقود ويجدّدها تلقائياً، وترتبط هوية كل عقدة بشهادتها مع رفض أي شهادة ملغاة أو قديمة.
- **ستة أدوار وموافقة شخصين من خطوتين:** يفصل النظام الصلاحيات عبر ستة أدوار (مشاهد، مشغّل، معتمِد، مدير نظام، مدقق، مدير مستأجر)، ويتطلّب موافقة شخصين مستقلين للعمليات الحساسة حيث يراجع المعتمِد الأثر أولاً ثم يكتب اسم الهدف، وترتبط الموافقة بالشخص الفعلي لا بالحساب.
- **هوية مؤسسية وسجل تدقيق بسلسلة تجزئة:** يتكامل النظام مع LDAP وActive Directory وOIDC وSAML والحسابات المحلية مع عامل ثانٍ مدمج TOTP يعمل في بيئة air-gap، ويحفظ الأسرار بتشفير المظروف ويمتلك سجل تدقيق غير قابل للتعديل مرتبطاً بسلسلة تجزئة وقابلاً للتصدير أو الإرسال إلى SIEM.
- **عزل المستأجرين وأمن التوريد:** يعزل النظام مهام كل مستأجر وطوابيره وبياناته ويقصر دخول SSH لعقدة الحساب على من لديه مهمة نشطة عليها، مع قفل الحزم وتوليد SBOM وبناء قابل لإعادة الإنتاج. التفاصيل الكاملة في صفحة الأمن.

الرصد والتنبيهات وتقارير الاستغلال

- **مصدّرات قياس قياسية وقواعد تنبيه:** يشتمل النظام على مصدّرات قياس بصيغة Prometheus القياسية لجميع العُقَد بما فيها العقدة الرئيسية، إلى جانب قواعد تنبيه ولوحات مراقبة مهيّأة مسبقاً.
- **العمل مع Prometheus وAlertmanager القائمة:** يتكامل النظام مع منظومة Prometheus وAlertmanager مع إمكانية تثبيت ملف تعريف المراقبة عبر المنتج، وتستطيع منظومتا Prometheus وGrafana القائمتان لدى المؤسسة قراءة البيانات ذاتها بينما تعمل لوحات المراقبة العميقة الأصلية داخل وحدة التحكم بالجلسة نفسها.
- **اختبار فعلي لسلسلة التنبيهات:** يتحقق النظام من مسار التنبيه كاملاً بإرسال تنبيه اختباري يصل إلى المناوب ويتطلّب تأكيد رمزه لإثبات جاهزية الاستجابة.
- **تقارير كفاءة الاستغلال:** يقدّم النظام تقارير استخدام تشمل نسبة معالجات GPU الخاملة في الأوقات التي تنتظر فيها مهام أخرى في الطابور.

تكامل التخزين المشترك وإدارة BMC

- **حماية نقاط ربط NFS وS3:** يدير النظام عملاء التخزين المشترك لأهداف NFS وS3، ويمنع الكتابة الصامتة على القرص المحلي للعقدة إذا لم يكن التخزين المشترك مربوطاً وسليماً.
- **ربط صحة التخزين بعرض الأثر:** تُراقَب حالة اتصال التخزين المشترك باستمرار وتُربَط بالمهام والمستأجرين المتأثرين ضمن عرض الأثر عند حدوث اضطراب.
- **قراءة بيانات BMC عبر Redfish:** يجمع النظام جرد العتاد وقراءات الحساسات وسجل أحداث النظام وحالة الطاقة من وحدات BMC المتوافقة مع معيار Redfish.
- **عمليات طاقة خاضعة للاعتماد:** لا تُنفَّذ عمليات الطاقة عبر BMC إلا كعمليات معتمدة دون تشغيل غير خاضع للرقابة.

أدوات سطر الأوامر للمشغّلين والباحثين

- **أداة المشغّل** `barestaxctl`: توفّر معاينة الخطط (`plan` و`dry-run`) وتقرير الفحص الشامل للعنقود (`doctor`) وتوليد حزمة الدعم الفني واختبار سلسلة التنبيهات وتشخيص العُقَد.
- **أداة الباحث** `barestax`: تتيح إرسال المهام ومتابعة حالتها وقراءة السجلات وإلغاء المهام ومراجعة الحصص واستعراض الصور المتاحة وقراءة أدلة التشغيل المحلية.

- **مخرجات مزدوجة للبشر والأتمتة:** تعرض الأداتان النتائج في جداول مقروءة للمستخدم أو بصيغة JSON منظّمة للتكامل مع النصوص والأنظمة البرمجية.

```
barestaxctl doctor
barestaxctl node diagnose gpu-07 --deep
barestax run -f job.yaml
barestax quota
barestax logs <job>
```

03

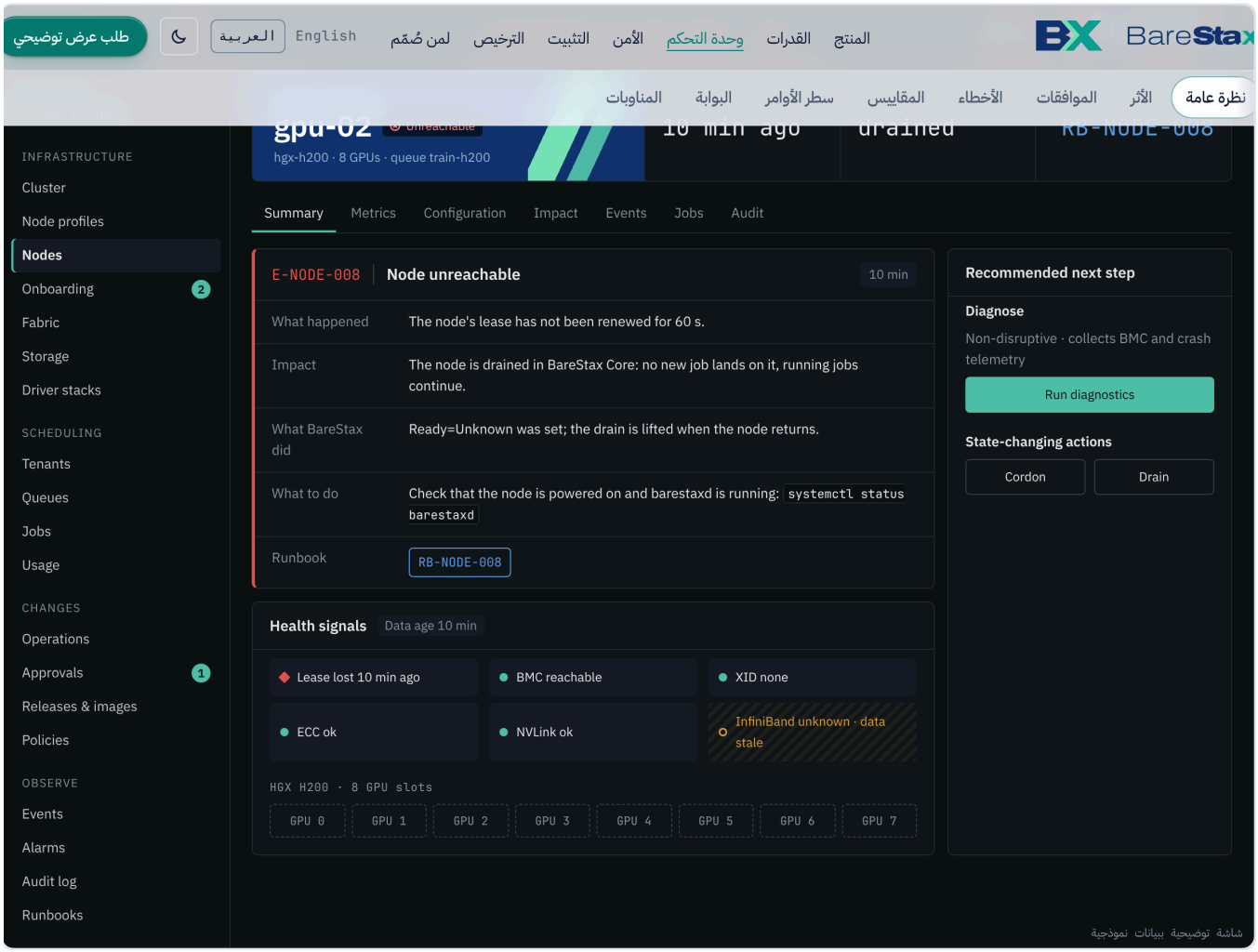
واجهة تشغيل واحدة للمشغّلين والباحثين دون اعتماد على الإنترنت

تعمل وحدة التحكم الرسومية على العقدة الرئيسية (head node) مدمجةً داخل الملف التنفيذي لمستوى التحكم (`barestax-server`)، بينما تُفتح بوابة الباحثين من عقدة الدخول (login node) بلغة التصميم ذاتها. تعرض الشاشات تغيّرات العنقود فور حدوثها، ولا تحتاج إلى أي موارد خارجية أو اتصال بالإنترنت.

ملخص العنقود والجرد وصفحات الكائنات السباعية

تجمع وحدة التحكم ملخص العنقود وجرد العتاد والعمليات والموافقات والتنبيهات والطوابير والحصص وطابور ترقية الصور وقارئ أدلة التشغيل في مكان واحد. وتُنظَّم صفحة كل كائن في العنقود عبر علامات تبويب تحمل أسماءها في واجهة المنتج: Summary, Metrics, Configuration, Impact, Events, Jobs, Audit.

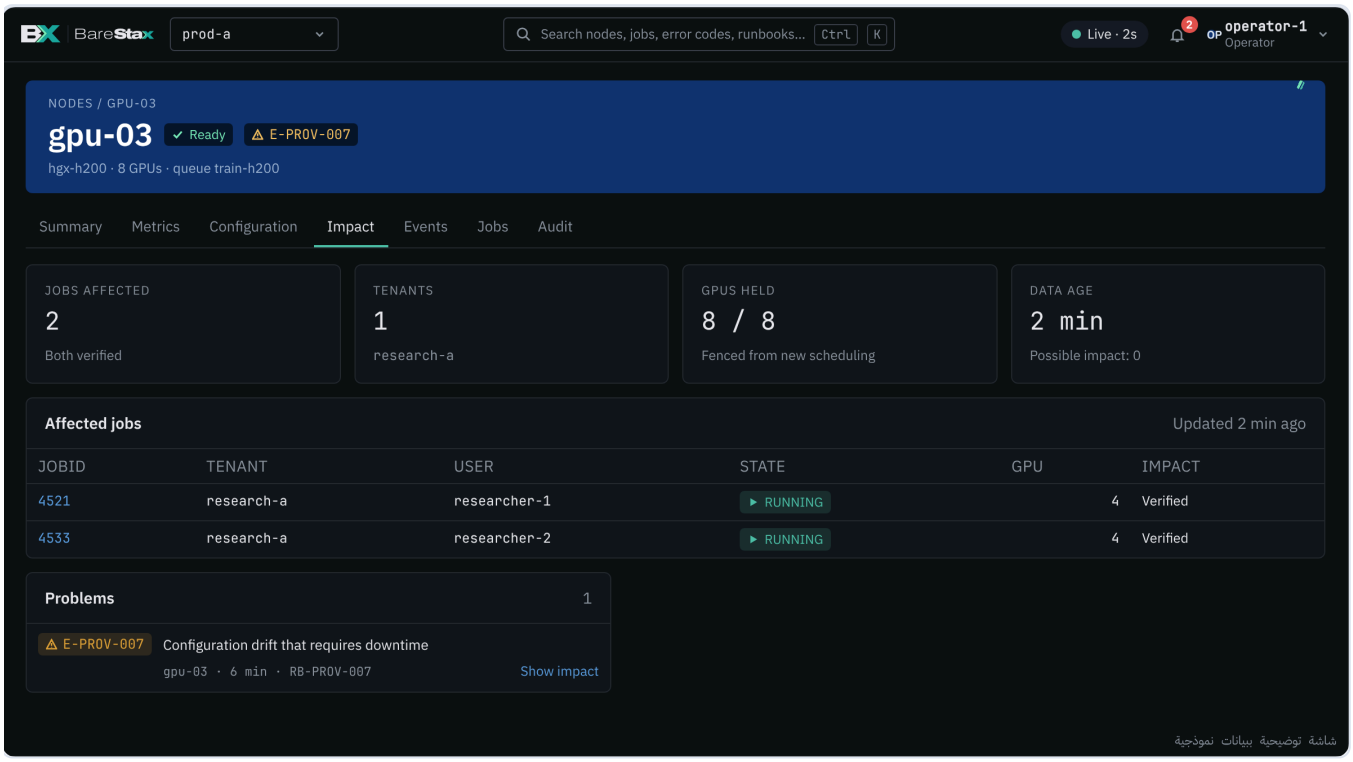
تتحدّث القراءات ببث حي من الخادم؛ فإذا انقطع الاتصال، تضع الواجهة وسم بيانات متقادمة بوضوح بدلاً من إبقاء أرقام قديمة توحي بأنها آنية.



صفحة عقدة في وحدة تحكم BareStax تعرض علامات التبويب وحالة العتاد والمهام النشطة وسجل الأحداث.

مسار متصل من التنبيه إلى عرض الأثر ثم الإجراء المعتمد

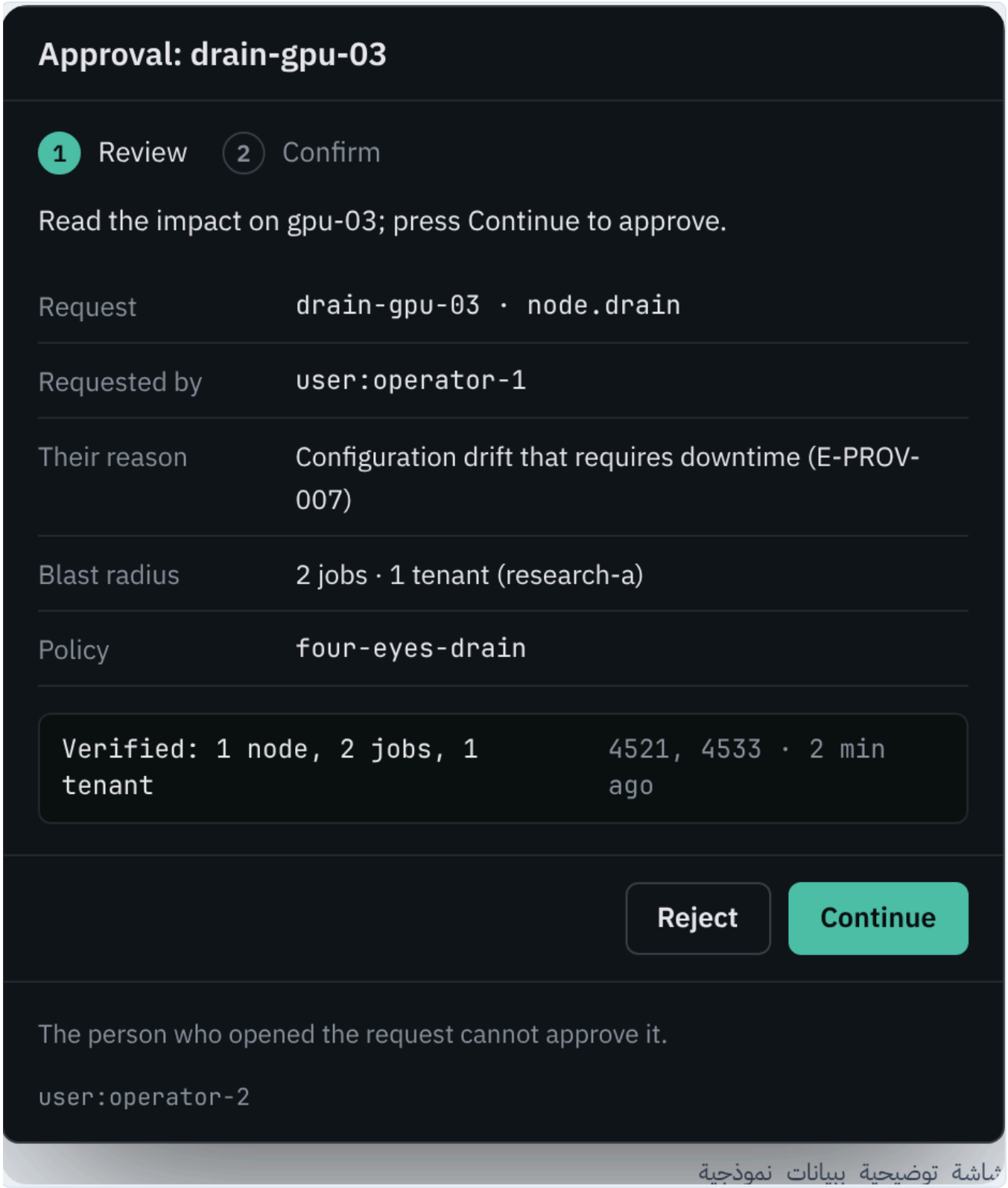
يقع عرض الأثر في مركز العمل التشغيلي داخل وحدة التحكم بدلاً من قوائم التنبيهات المنعزلة عن سياقها. عند اختيار أي تنبيه أو عقدة أو هدف تخزين، يظهر فوراً نطاق المهام والمستأجرين والخدمات المتأثرة مع التمييز بين الأثر المؤكد والمحتمل وبيان عمر البيانات. ومن الشاشة ذاتها يبدأ المشغّل الإجراء التصحيحي المناسب ويرسله للاعتماد.



شاشة عرض الأثر تربط التنبيه النشط بالمهام والمستأجرين المتأثرين وتفتح مسار طلب الإجراء المعتمد.

موافقة شخصين من خطوتين تصعّب اعتماد الهدف الخاطئ

تفرض نافذة الاعتماد في وحدة التحكم موافقة شخصين (أربع أعين) على الإجراءات الحساسة عبر خطوتين متتاليتين؛ إذ يعاين المعتمِد أولاً الأثر الفعلي للعملية، ثم يكتب اسم الهدف يدوياً لتأكيد القصد مع إعادة التحقق عبر العامل الثاني TOTP. وترتبط الموافقة بالشخص الفعلي لا بالحساب المشترك، ولا يستطيع مقدّم الطلب اعتماد طلبه الشخصي.

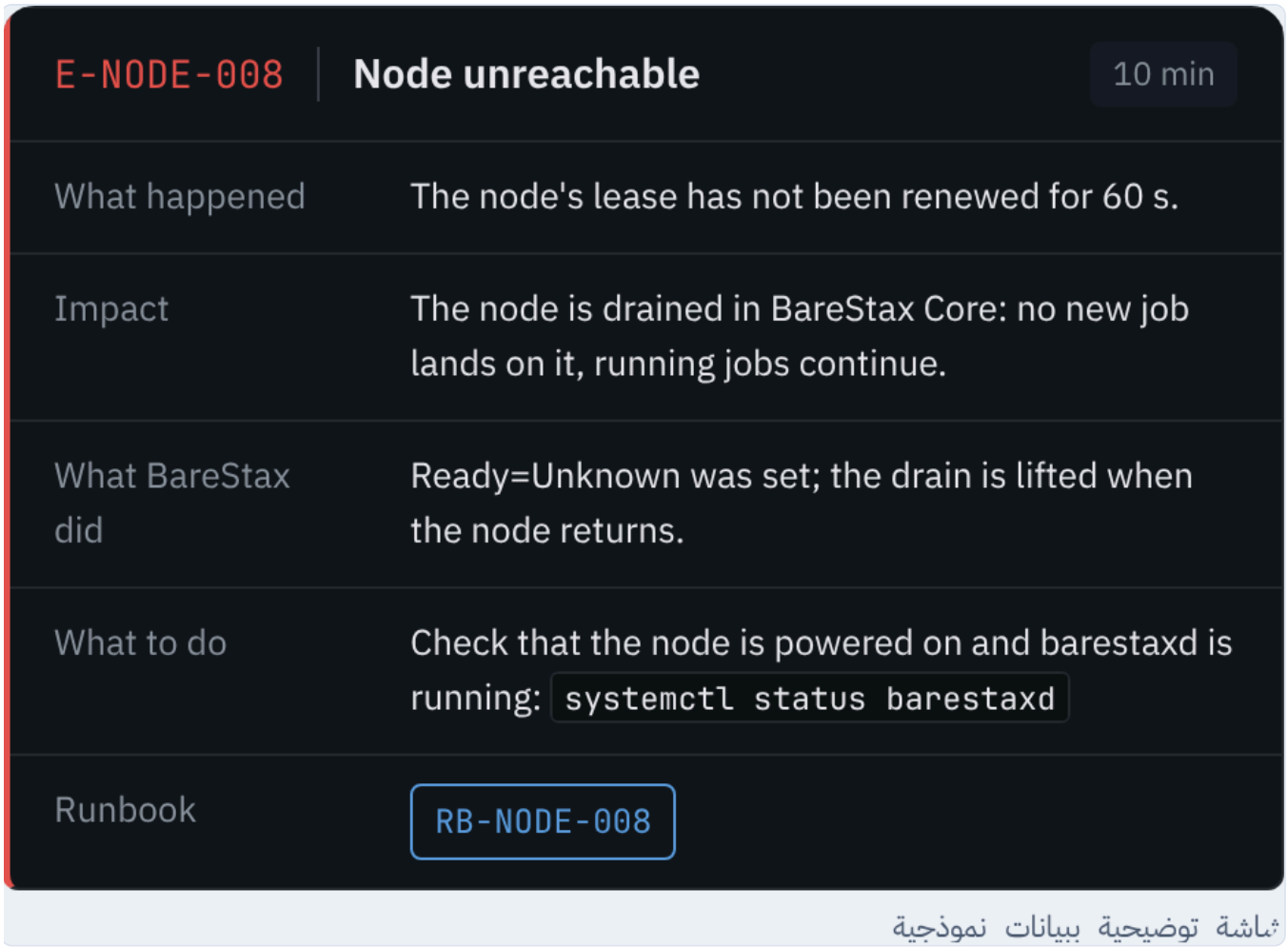


شاشة توضيحية ببيانات نموذجية

نافذة اعتماد من خطوتين لعملية تفريغ عقدة تعرض الأثر أولاً ثم تطلب كتابة اسم الهدف من معتمِد مستقل عن مقدّم الطلب.

أخطاء مرمّزة من خمسة أقسام مربوطة بأدلة تشغيل محلية

يحمل كل خطأ رمزاً تعريفياً ثابتاً ويُعرَض في بطاقة من خمسة أقسام: ماذا حدث، الأثر الحالي، ما الذي قام به المنتج تلقائياً، ما الإجراء المطلوب من المشغّل، ورابط دليل التشغيل (runbook). وتعمل جميع أدلة التشغيل محلياً داخل وحدة التحكم دون اتصال بالإنترنت.

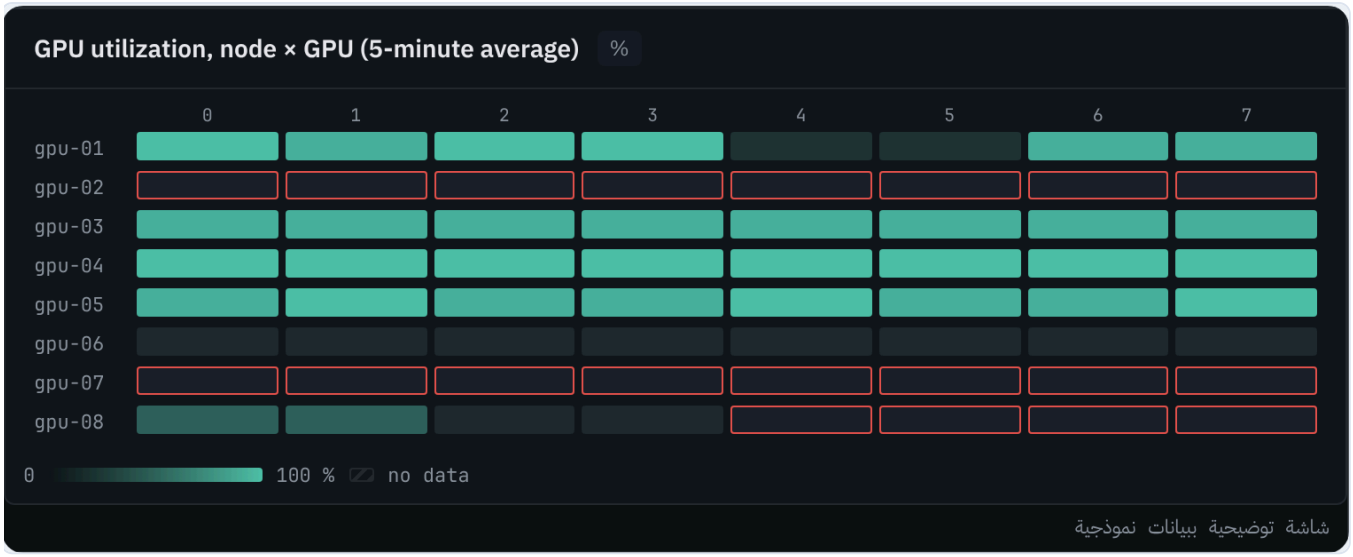


شاشة توضيحية ببيانات نموذجية

بطاقة خطأ مرمّز توضح الأقسام الخمسة التفسيرية وتفتح دليل التشغيل المحلي المرتبط بالرمز.

خريطة حرارية للعنقود ولوحات مراقبة عميقة في الجلسة ذاتها

تعرض الخريطة الحرارية مصفوفة العُقَد ومعالجات GPU على مستوى العنقود بالكامل على مستوى العنقود. وترافقها رسوم بيانية لإشغال GPU والذاكرة واستهلاك الطاقة والحرارة وحركة الشبكة، إلى جانب لوحات مراقبة عميقة خاصة بالمنتج تُفتح داخل وحدة التحكم وبالجلسة نفسها دون تسجيل دخول منفصل.



شاشة توضيحية ببيانات نموذجية

الخريطة الحرارية للعنقود تعرض مصفوفة العُقَد ومعالجات GPU ومستويات الإشغال والحرارة في شاشة واحدة.

تكافؤ كامل بين الواجهة الرسومية وسطر الأوامر

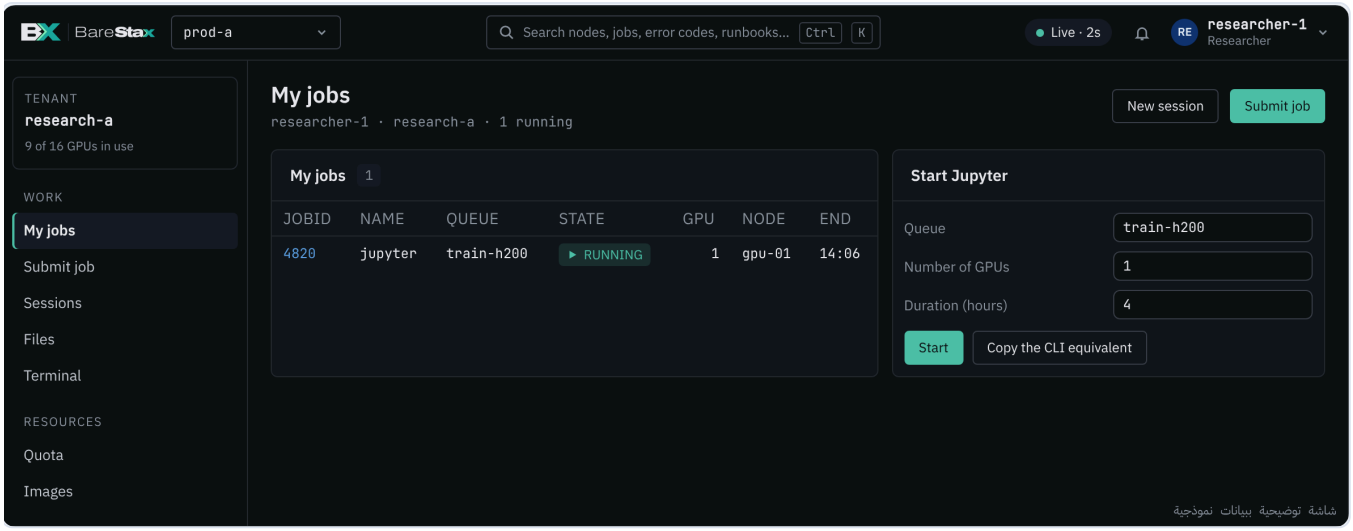
توفّر وحدة التحكم مقابل كل إجراء أمر سطر الأوامر المكافئ له جاهزاً للنسخ المباشر، وتستخدم الواجهة الرسومية وأداتا `barestaxctl` و`barestax` الواجهة البرمجية نفسها.

```
barestaxctl operation list
barestaxctl operation approve <name>
barestax status
barestax runbook RB-NODE-008
```

بوابة الباحثين من عقدة الدخول بالهوية الفعلية للمستخدم

تُفتح بوابة الباحثين من عقدة الدخول بالتصميم الموحّد ذاته؛ وفي شاشة My jobs يراجع الباحث حالة كل مهمة وسبب انتظارها وسجلها وخيار إلغائها إلى جانب حصته المتاحة، كما يرسل مهام جديدة عبر نماذج القوالب.

تُطلَق الجلسات التفاعلية لبيئات Jupyter وVS Code وRStudio وسطح المكتب البعيد كمهام BareStax Core نظامية وتُفتح في المتصفح. يقتصر الوصول إلى الجلسة على مالكها فقط، وتُغلَق الجلسات الخاملة تلقائياً لتحرير معالجات GPU، بينما يعمل مدير الملفات والطرفية في المتصفح ومساحة العمل الدائمة بالهوية الفعلية للمستخدم على Linux.



بوابة الباحثين تعرض قائمة المهام وأسباب الانتظار وحصة المستخدم وإطلاق جلسات Jupyter وVS Code عبر المتصفح.

واجهة إنجليزية وتنقل كامل بلوحة المفاتيح

واجهة وحدة التحكم وبوابة الباحثين باللغة الإنجليزية فقط، مع دعم السمة الداكنة والسمة الفاتحة، والتنقل الكامل عبر لوحة المفاتيح ولوحة الأوامر.

04

الأمن جزء من آلية التشغيل نفسها لا طبقة مضافة لاحقاً

بُنيت الضوابط الأمنية في BareStax داخل مسار انضمام العُقَد وتشغيل المهام وتوزيع التحديثات منذ اللحظة الأولى. تخضع هوية كل عقدة ومصدر كل صورة حاوية للتحقق التشفيري، وتُحدَّد صلاحية كل مشغّل بدوره، سواء عمل العنقود في شبكة متصلة أو في شبكة معزولة عن الإنترنت (air-gap).

هوية العُقَد والمستخدمين عبر mTLS ومزوّدي الهوية المؤسسية

تُنشَأ كل قناة اتصال داخل العنقود عبر بروتوكول TLS المتبادل (mTLS) بالاعتماد على بنية المفاتيح العامة PKI الخاصة بالعنقود نفسه. يجدّد النظام الشهادات، ويبادر وكيل العقدة `barestaxd` بالاتصال بمستوى التحكم بنفسه، فلا تتلقى العُقَد أوامر من الخارج. وترتبط هوية كل عقدة حساب بشهادتها؛ فلا تُقبَل أي شهادة ملغاة أو قديمة، وتُبطَل الهوية القديمة للعقدة فور إخراجها حتى لو أُعيد ضمّها لاحقاً بالاسم ذاته.

على مستوى المستخدمين، يتكامل BareStax مع أدلة المؤسسة عبر LDAP وActive Directory ومع موفّري الهوية المؤسسية عبر OIDC وSAML إلى جانب الحسابات المحلية. ويوفّر النظام مصادقة عامل ثانٍ مدمجة عبر TOTP تعمل محلياً بالكامل في الشبكات المعزولة عن الإنترنت، مع إعادة طلب العامل الثاني قبل تنفيذ أي عملية حرجة.

تُحفَظ الأسرار داخل النظام باستخدام تشفير المظروف (envelope encryption)، وتُخزَّن كلمات المرور بصيغ تجزئة تشفيرية حديثة، وتشمل النسخة الاحتياطية لمستوى التحكم الهوية وبنية PKI وقاعدة البيانات وحالة BareStax Core مع عزل العقدة الرئيسية القديمة بعد الاستعادة لمنعها من الاستجابة.

ستة أدوار محدّدة وموافقة شخصين مرتبطة بالأفراد

يعمل التحكم بالوصول المبني على الأدوار عبر ستة أدوار في وحدة التحكم الرسومية وأداة `barestaxctl` : المشاهد، المشغّل، المعتمِد، مدير النظام، المدقق، ومدير المستأجر.

تتطلّب العمليات الحرجة مثل إخراج عقدة حساب أو ترقية صورة حاوية أو إعادة إقلاع خادم موافقة شخصين (أربع أعين) من فردين مختلفين. وتتم الموافقة على خطوتين؛ إذ يرى المعتمِد أولاً الأثر الفعلي للعملية، ثم يكتب اسم الهدف لتأكيده بحيث يصعب اعتماد هدف خاطئ. ولا يستطيع مقدّم الطلب اعتماد طلبه بنفسه. وترتبط الموافقة بالشخص لا بالحساب.

تُنفَّذ عمليات الطاقة عبر BMC كعمليات معتمدة فقط، وتحدد السياسة أي خطوات الاسترداد تعمل تلقائياً وأيها يحتاج اعتماداً.

```
barestaxctl operation list
barestaxctl operation approve <name>
```

سجل تدقيق غير قابل للتعديل مرتبط بسلسلة تجزئة

سجلات التدقيق في BareStax غير قابلة للتعديل، إذ يرتبط كل سجل بما يسبقه عبر سلسلة تجزئة تشفيرية (hash chain). ويمكن تصدير سجلات التدقيق للمراجعة أو إرسالها إلى أنظمة SIEM المعتمدة لدى المؤسسة، كما تتوفّر علامة التبويب Audit ضمن صفحات الكائنات في وحدة التحكم.

عزل صارم بين المستأجرين وتشغيل حصري للصور الموقّعة

يفصل BareStax بين المستأجرين على مستوى الطوابير والحصص والمهام والبيانات، فلا يتمكّن أي مستأجر من رؤية مهام مستأجر آخر أو طوابيره أو بياناته. وعلى مستوى عُقَد الحساب، لا يُفتح اتصال SSH إلا للمستخدم الذي يمتلك مهمة جارية على تلك العقدة تحديداً مع استثناء قابل للضبط لمديري النظام، بينما تنفَّذ عمليات مدير الملفات والطرفية في بوابة الباحثين بالهوية الفعلية للمستخدم على Linux.

تعمل جميع أحمال العمل داخل حاويات Apptainer للقراءة فقط دون تشغيل Docker على العُقَد، بينما تُحفَظ الحزم وذاكرة النماذج المؤقتة في مساحة العمل الدائمة للمستخدم دون تعديل الصورة الأساسية. وتستورد المؤسسة الصور إلى سجل OCI المدمج لفحصها وترقيتها بموافقة شخصين وتوقيعها بمفتاح العنقود مع دعم سجل المؤسسة الخاص والتوقيع المقابل للمؤسسة، وترفض عُقَد الحساب بدء أي صورة غير موقّعة أو غير معتمدة.

سلسلة توريد برمجية قابلة للتحقق وبناء قابل لإعادة الإنتاج

تُولَّد مفاتيح توقيع الإصدارات في بيئة غير متصلة بالشبكة ضمن مراسم مفاتيح مسجّلة. وتُثبَّت المستودعات المصدرية بلقطات زمنية محددة مع حفظ بصمات مفاتيحها داخل قسم الثقة في حزمة الإصدار، بحيث ينتج الإصدار الواحد البايتات ذاتها في كل عملية تثبيت وتثبّت العُقَد حزمها من المستودع المحلي للعنقود فقط.

تُبنى برمجيات المنتج بأسلوب قابل لإعادة الإنتاج (reproducible build) مع قفل الحزم وتوليد قائمة مكوّنات البرمجيات SBOM وتطبيق قائمة سماح صريحة للتراخيص.

تشغيل كامل دون إنترنت ودون الاتصال بخادم بعيد

يعمل BareStax داخل مركز بيانات المؤسسة حصراً، فلا يرسل أي بيانات إلى الخارج ولا يتصل بأي خادم بعيد. تعبر حزم الإصدار الموقّعة حد العزل عبر وسائط نقل معتمدة أو الصمام الثنائي للبيانات (data diode) ولا تُنشَر إلا بعد فحص التوقيع والسلامة والتوافق وموافقة شخصين. ويعمل الترخيص محلياً دون خادم تراخيص خارجي، كما تعمل وحدة التحكم (واجهتها باللغة الإنجليزية فقط) وأدلة التشغيل المحلية (runbooks) وبوابات الصحة المحلية على العُقَد دون أي حاجة إلى الإنترنت.

05

متطلبات واضحة ومسار تثبيت موحّد للشبكات المتصلة والمعزولة

يركّب BareStax فوق نظام Ubuntu 24.04 LTS الذي تثبّته المؤسسة وفق معاييرها المعتمدة دون مسح الأقراص أو فرض أداة إقلاع شبكي. يتبع التثبيت والتحديث المسار ذاته من ملف التعريف الصغير (2–4 عُقَد GPU) إلى ملف التعريف القياسي (5–128 عقدة GPU، وبحد أقصى 1,024 معالج GPU).

متطلبات العتاد والشبكة وملفات تعريف الحجم

يدعم النظام التشكيلات العتادية والبرمجية التالية في مراكز البيانات المؤسسية:

- **معالجات GPU:** معالجات NVIDIA من فئتي مراكز البيانات ومحطات العمل، بما يشمل أنظمة HGX من جيلي Hopper وBlackwell والخوادم المزوّدة ببطاقات PCIe GPU. تعمل الفئات المختلفة جنباً إلى جنب في حوض واحد بطوابير مستقلة، وتُنشر قائمة الفئات العتادية المتحقّق منها في ملاحظات كل إصدار.
- **النسيج الشبكي:** شبكات InfiniBand وRoCE وروابط NVLink وNVSwitch؛ وهذه الروابط غير إلزامية، إذ تنضم الخوادم المزوّدة بشبكة Ethernet فقط إلى العنقود وتعمل بصورة طبيعية.
- **نظام التشغيل:** توزيعة Ubuntu 24.04 LTS لمعمارية amd64 مثبتة من قِبل المؤسسة، ويحافظ BareStax على إعداد التثبيت الأصلي وتقسيم الأقراص ويثبّت النواة المعتمدة بعد الانضمام.
- **التخزين المشترك وBMC:** أهداف تخزين خارجية عبر NFS وS3 مع حماية نقاط الربط لمنع الكتابة الصامتة على القرص المحلي عند غياب التخزين (ولا يتولّى BareStax إنشاء خادم التخزين نفسه)، ووحدات إدارة BMC المتوافقة مع معيار Redfish لقراءة الجرد والحساسات وسجل الأحداث وحالة الطاقة مع تنفيذ عمليات الطاقة كعمليات معتمدة فقط.

ملف التعريف	نطاق عُقَد GPU	السقف الأقصى لمعالجات GPU	متطلب العقدة الرئيسية (head node)
صغير	2–4 عُقَد GPU	حسب عدد المعالجات في العُقَد	خادم دون GPU أو آلة افتراضية مستقلة
قياسي	5–128 عقدة GPU	1,024 GPU	عقدة رئيسية مخصّصة ومستقلة

خطوات التأسيس في اليوم 0 واليوم 1

تكتمل تهيئة العنقود وضم أولى عُقَد الحساب عبر أربع خطوات متسلسلة:

1. تثبيت مستوى التحكم على العقدة الرئيسية بأمر واحد مع حفظ نسخة احتياطية لمفاتيح العنقود في الملف المحدد.
2. ربط الهوية المؤسسية (LDAP أو Active Directory أو OIDC أو SAML أو الحسابات المحلية) وتفعيل العامل الثاني TOTP وتعريف الشبكة وأهداف التخزين NFS وS3.
3. اختبار سلسلة التنبيهات من الطرف إلى الطرف للتثبّت من وصول تنبيه الاختبار إلى المناوب وتأكيد رمزه فعلياً.
4. إجراء فحوص ما قبل الانضمام للبرمجيات الثابتة والأقراص وSecure Boot والاتصال على خادم Ubuntu 24.04 LTS، ثم توليد رمز انضمام وتنفيذ أمر واحد واعتماد العقدة بموافقة واحدة لجرد العتاد ومطابقة ملف التعريف وتثبيت المكدس المتوافق واجتياز فحوص GPU وNVLink وInfiniBand وNCCL بين عقدتين قبل إدراجها في BareStax Core.

```
barestax-server init --cluster-name <name> --endpoint <fqdn> --key-backup <file>
barestaxctl token create
barestaxd join --token-file <path>
barestaxctl node approve gpu-03
```

تدفق حزم الإصدار في الشبكات المعزولة عن الإنترنت

في البيئات المعزولة عن الإنترنت (air-gap)، يتولّى `barestax-bundler` على الطرف المتصل بالإنترنت جمع النواة والتعريفات ومكتبات CUDA وNCCL وحزم النظام والصور في حزمة إصدار مفهرسة بالمحتوى وموقّعة رقمياً بمفاتيح وُلدت ضمن مراسم مفاتيح غير متصلة بالشبكة. وتُثبَّت المستودعات المصدرية بلقطات زمنية مع حفظ بصمات مفاتيحها داخل قسم الثقة في الحزمة، ثم تُنقل الحزمة عبر وسائط نقل محمولة معتمدة أو عبر الصمام الثنائي للبيانات (data diode).

عند استيراد الحزمة إلى مستوى التحكم، يفحص النظام التوقيع الرقمي وسلامة المحتوى والتوافق مع العنقود ويرفق تقرير الفحص الأمني. وبعد صدور موافقة شخصين (أربع أعين)، تبدأ الترقية بعقدة واحدة أولاً ثم تمتد إلى بقية العُقَد ومستوى التحكم ضمن ميزانية التوقف المحددة ودون قطع المهام الجارية.

```
barestax-bundler export
barestax-bundler verify
barestaxctl release import <bundle>
barestax-server upgrade --offline
```



مخطط تدفق حزمة الإصدار عبر حد العزل من التجميع والتوقيع إلى التحقق وموافقة شخصين والترقية المرحلية.

سياسة الترقية والدعم لمدة 24 شهراً لكل خط إصدار

يحظى كل خط إصدار فرعي بدعم فني وتحديثات أمنية لمدة 24 شهراً تبدأ من تاريخ إطلاقه العام الأول. وتصل التصحيحات الأمنية كحزم إصدار موقّعة تنتج البايتات ذاتها في كل بيئة لتطبّقها المؤسسة ضمن نوافذ الصيانة وميزانية التوقف المعتمدة لديها.

06

ترخيص بسيط لبنية تحتية سيادية

وحدة ترخيص واحدة، واشتراك سنوي واحد، وملف ترخيص موقّع يعمل دون اتصال. لا يعتمد عنقودكم على أي اتصال بنا.

الشروط في خمسة أسطر

الترخيص لكل عقدة GPU

كل عقدة حساب فيها GPU وحدة ترخيص واحدة، ولا تُحتسب العقدة الرئيسية وعقدة الدخول وعقدة البناء. فئتان للعُقَد: عُقَد من 1 إلى 4 وحدات GPU، وعُقَد من 5 إلى 8 وحدات GPU، دون فرق بحسب جيل GPU. يبدأ الترخيص من عقدتي GPU.

اشتراك لا يوقف العنقود

الترخيص اشتراك سنوي. وإذا لم تجدّدوا يبقى آخر إصدار مستورد والسعة المرخّصة في الخدمة، وتستمر المهام والتفريغ والتعافي. ويشمل التجديد الإصدارات الجديدة والدعم وتغييرات السعة.

ملف ترخيص لا خادم تراخيص

الترخيص ملف موقّع يُثبَّت دون اتصال. لا خادم تراخيص ولا اتصال صادر ولا قياس عن بُعد.

24 شهراً لكل خط إصدار

يُدعم كل خط إصدار فرعي لمدة 24 شهراً من أول إتاحة عامة. وتصل إصلاحات الأمن على هذا الخط حزمَ إصدار موقّعة، عبر المسار نفسه الذي تستخدمونه في الشبكة المعزولة.

الدعم القياسي مشمول

الدعم القياسي جزء من الاشتراك. تُعالج الطلبات وفق ثلاثة مستويات أولوية، وتُحدَّد أهداف الاستجابة والحل في اتفاقية الدعم.

عرض توضيحي أولاً ثم تجربة مدفوعة

أثبتوا BareStax على عتادكم قبل أي التزام.

1. **عرض توضيحي:** جلسة عن بُعد على المنتج، مبنية على أسئلة فريقكم.
2. **جلسة تقنية:** العتاد والنسيج الشبكي والتخزين والهوية وطريقة النقل.
3. **تجربة مدفوعة:** عقدة رئيسية منفصلة وحتى 4 عُقَد GPU لمدة 90 يوماً، تبدأ عندما يصبح العتاد جاهزاً.
4. **تدريبات القبول:** انضمام عقدة، والفحص بين عقدتين، وتحديث يبدأ بعقدة واحدة، والتفريغ والتعافي، والاستيراد في شبكة معزولة، وتصدير سجل التدقيق، واستعادة مستوى التحكم.
5. **طلب الإنتاج:** ترخيص التجربة محدد المدة. وإذا طلبتم الإنتاج خلال 60 يوماً تُحتسب رسوم التجربة كاملةً من السنة الأولى.

قائمة اختبارات قبول التجربة

كيف يُبنى عرض السعر

نقدّم عرض السعر بعد مناقشة نطاق العنقود واحتياجات الدعم. ويُبنى على:

- عدد عُقَد GPU وفئتها، من 1 إلى 4 أو من 5 إلى 8 وحدات GPU؛
- احتياجات الدعم لديكم؛
- التجربة، إن بدأتم بها.

يستطيع فريقكم مراجعة النظرة العامة التقنية وقائمتي التحقق قبل أي التزام. الموارد

07

صُمّم للمؤسسات التي تملك وحدات GPU الخاصة بها

صُمّم BareStax للمؤسسات التي تشغّل عناقيد NVIDIA GPU في مراكز بياناتها وتحتاج إلى إبقاء البيانات والمفاتيح والتشغيل تحت سيطرتها: فرق الذكاء الاصطناعي في الشركات، ومراكز الأبحاث والجامعات، والجهات الحكومية، والقطاعات الخاضعة للتنظيم مثل المال والصحة والاتصالات والطاقة.

حسب القطاع

المؤسسات العامة

عناقيد تبقى داخل المؤسسة: لا اتصال صادر، وملف ترخيص يعمل دون اتصال، ومفاتيح العنقود وسجل التدقيق داخل مركز بياناتكم، وشخصان في كل عملية حرجة.

مراكز الأبحاث والجامعات

وحدات GPU مشتركة بين مجموعات كثيرة: مستأجرون وحصص وتوزيع عادل ومحاسبة، مع بوابة لجلسات Jupyter وVS Code وRStudio وسطح المكتب البعيد. تُغلق الجلسات الخاملة وتُحرَّر وحدة GPU.

المال والصحة والاتصالات والطاقة والصناعة

أدلة يستطيع المدققون فحصها: سجل تدقيق مرتبط بسلسلة تجزئة يمكن تصديره إلى نظام SIEM، وصور حاويات موقّعة ومعتمدة فقط، وقائمة مكوّنات البرمجيات (SBOM) وقفل الحزم في سلسلة التوريد، وعزل المستأجرين.

مقارنة الأساليب

الأسلوب	نقطة القوة	ما يبقى على فريقكم
مدير عناقيد ونصوص برمجية	أدوات تثبيت ناضجة	الترقيات والتعافي وإجراءات العزل يدوية، وخطأ في ترتيب النصوص قد يترك تثبيتاً ناقصاً دون إنذار.
Kubernetes مع مشغّل GPU	قوي لأحمال الخدمات	طبقات جدولة وRDMA إضافية لتدريب الدفعات، ويبقى نظام التشغيل وبرامج التشغيل والنسيج وBMC خارجه.
طبقة افتراضية مع تمرير PCIe	تشغيل مألوف للآلات الافتراضية	تبقى وحدة GPU مرتبطة بالآلة الافتراضية وخاملة بخمولها، دون مشاركة بين المهام.
BareStax	منتج واحد من الخادم في الرف إلى طابور المهام، تصريحي وذاتي الإصلاح ومعزول من طرف إلى طرف	تركيب العتاد وتثبيت Ubuntu.

ما ليس BareStax

ليس توزيعة Kubernetes ولا منصة أجهزة افتراضية ولا خدمة سحابية. يعمل في مركز بياناتكم ولا يرسل أي بيانات إلى الخارج، ولا يثبّت نظام التشغيل ولا يوفّر التوسّع التلقائي ولا موازنة الحمل؛ يوفّر موازن الحمل لديكم الوصول إلى الخدمات طويلة التشغيل.

08

إجابات تقنية واضحة حول بنية BareStax وتشغيله

تفاصيل معمارية وتشغيلية حول العلاقة مع Kubernetes والمحاكاة الافتراضية، العتاد المدعوم، تحديثات بيئات air-gap، جدولة المهام، ضوابط الأمن، وسياسة الترخيص والدعم.

البنية التحتية

هل يضع BareStax طبقة Kubernetes فوق عنقود GPU؟

لا، فنظام BareStax ليس توزيعة Kubernetes ولا يشغّل Kubernetes فوق عُقَد الحساب. يطبّق النظام النموذج التصريحي ذاتي الإصلاح على النواة والتعريفات ونسيج NVLink وInfiniBand ووحدات BMC وجدولة المهام، فتصل المهام مباشرة إلى العتاد دون طبقات وسيطة.

هل يعتمد النظام على المحاكاة الافتراضية أو تقسيم MIG وvGPU؟

لا يستخدم BareStax المحاكاة الافتراضية على عُقَد GPU ولا يقسّم المعالجات عبر MIG أو vGPU. يُخصَّص كل معالج GPU بالكامل للمهمة الجارية عبر BareStax Core ويُحرَّر فور انتهائها ليُسنَد إلى المهمة التالية، بينما يمكن تشغيل العقدة الرئيسية الخالية من GPU على خادم فيزيائي أو داخل آلة افتراضية على منصة المؤسسة.

هل يثبّت BareStax نظام التشغيل من الصفر أو يمسح أقراص الخوادم؟

لا، إذ تثبّت المؤسسة نظام Ubuntu 24.04 LTS لمعمارية amd64 وفق معاييرها وتقسيماتها المعتمدة للأقراص. يحافظ BareStax على نظام التشغيل القائم ولا يمسح الأقراص، ثم يتولّى تثبيت النواة المعتمدة والتعريفات ومكدس الحوسبة وإدارتها تصريحياً بعد الانضمام.

ما فئات معالجات GPU والشبكات المدعومة؟

يعمل النظام مع فئتي مراكز البيانات ومحطات العمل من معالجات NVIDIA، شاملاً منصات HGX بجيلي Hopper وBlackwell وخوادم PCIe GPU وفق القائمة المتحقّق منها في ملاحظات الإصدار. وتُدعَم شبكات InfiniBand وRoCE وروابط NVLink وNVSwitch، كما تنضم الخوادم المزوّدة بـ Ethernet فقط دون اشتراط نسيج عالي السرعة؛ وترد المتطلبات الكاملة في صفحة التثبيت.

ما أحجام العناقيد المدعومة وما متطلبات العقدة الرئيسية؟

يتوفّر ملفا تعريف للحجم: ملف التعريف الصغير من 2 إلى 4 عُقَد GPU، وملف التعريف القياسي من 5 إلى 128 عقدة GPU وبسقف يصل إلى 1,024 معالج GPU. ويعمل ملف التعريف القياسي بعقدة رئيسية (head node) مستقلة ومخصّصة، ويمكن أن تكون خادماً دون GPU أو آلة افتراضية.

التشغيل

كيف يتم الانتقال من عنقود قائم إلى BareStax؟

لا يستورد BareStax إعدادات المجدول القائم في موضعها، بل يولّد إعدادات BareStax Core الخاصة به ويوزّعها تلقائياً مع محاسبة المهام. يتم الانتقال خادماً تلو الآخر عبر ضم كل خادم مع الحفاظ على تثبيت Ubuntu 24.04 LTS القائم عليه، وتُعرَّف الطوابير والمستأجرون والحصص وسياسة fairshare داخل BareStax بينما يرسل الباحثون مهامهم عبر سطر الأوامر أو القوالب أو البوابة. ويُخطَّط ترتيب نقل الخوادم بصورة مشتركة وفق عتاد المؤسسة وبنية طوابيرها.

ماذا يحدث عند تعطل عقدة حساب أثناء تشغيل المهام؟

تتوقف العقدة المتعطلة عن استقبال مهام جديدة (drain) مع الحفاظ على المهام الجارية عليها حتى تكتمل، وتمنع آلية الحماية من التذبذب إخراج العقدة بسبب إشارات عابرة. وتُعاد جدولة المهام المُرسَلة عبر قوالب `barestax run` في الطابور بأمان عند تعطل العقدة. ويسير الاسترداد المتدرج من إعادة تشغيل الخدمة إلى إعادة إقلاع النظام ثم دورة الطاقة عبر BMC وفق ما تحدده السياسة من خطوات تلقائية أو معتمدة، مع توقف السلسلة تلقائياً عبر مكبح العواصف عند الأعطال الجماعية.

كيف تتم إزالة عقدة من العنقود للصيانة أو الاستبدال؟

تُفرَّغ العقدة أولاً من المهام (`barestaxctl node drain`) بحيث لا يضيع أي عمل قيد التنفيذ، وتتطلّب إزالتها النهائية (`barestaxctl node remove`) موافقة شخصين (أربع أعين) يعاين فيها المعتمِد الأثر أولاً ثم يكتب اسم العقدة المستهدفة. وعقب الإزالة تُبطَل هوية الشهادة السابقة للعقدة فوراً، مع إمكانية إعادة ضمّها لاحقاً بالاسم ذاته بهوية جديدة.

كيف تعمل الخدمات طويلة الأمد مثل خوادم النماذج؟

تُشغَّل خوادم النماذج وسائر الخدمات المستمرة ضمن طابور مستقل في BareStax Core مع تسجيل الخدمة وحمايتها. أمّا استقبال الطلبات القادمة من خارج العنقود فيتم عبر موازن الحمل الخاص بالمؤسسة، نظراً لعدم تضمين موازنة حمل شبكية أو تحجيم تلقائي في المنتج؛ وتفاصيل ذلك في صفحة القدرات.

ماذا يحدث للمهام الجارية إذا توقّف مستوى التحكم؟

تستمر المهام الجارية على عُقَد الحساب دون انقطاع؛ إذ تبقى كل عقدة على آخر حالة آمنة معروفة وتمنع بوابة الصحة المحلية إسناد أعمال جديدة لأي عقدة متعطلة. وعند الحاجة يُستعاد مستوى التحكم بكامل بياناته وشهاداته وحالة BareStax Core من النسخة الاحتياطية على خادم نظيف مع حجب الخادم القديم، وترد تفاصيل الاستمرارية في صفحة المنتج.

كيف يعرف الباحث سبب انتظار مهمته وحالة حصته؟

تعرض بوابة الباحثين وأمر `barestax quota` وأمر `barestax status` الحصة المتاحة والمستهلكة والسبب الفعلي لانتظار المهمة في طابور BareStax Core. وبذلك يتحقق الباحث بنفسه مما إذا كان الانتظار راجعاً إلى الحصة أو أولوية fairshare أو انشغال فئة GPU المطلوبة.

كيف يتكامل BareStax مع Grafanag Prometheus؟

يضم BareStax مصدّرات قياس مدمجة لجميع العُقَد بما فيها العقدة الرئيسية وقواعد تنبيه ولوحات جاهزة، ويتكامل مع Prometheus وAlertmanager مع إمكانية تثبيت ملف تعريف المراقبة عبر المنتج. وتعمل المصدّرات بصيغة Prometheus القياسية، فيمكن لمنظومتي Prometheus وGrafana القائمتين لدى المؤسسة قراءة البيانات ذاتها. أمّا الخريطة الحرارية ولوحات المراقبة العميقة فهي لوحات أصلية خاصة بالمنتج تُفتح داخل وحدة التحكم بالجلسة ذاتها، وليست لوحات Grafana مدمجة داخل وحدة التحكم.

الأمان

كيف تُنفَّذ التحديثات في الشبكات المعزولة عن الإنترنت (air-gap)؟

تجمّع أداة `barestax-bundler` على الطرف المتصل بالإنترنت حزمة إصدار مفهرسة بالمحتوى وموقّعة رقمياً تضم الحزم وبرامج التشغيل والصور، وتُجمَّد المستودعات المصدرية بلقطات زمنية ثابتة. تُنقل الحزمة عبر وسائط نقل معتمدة أو الصمام الثنائي للبيانات (data diode) إلى داخل الشبكة المعزولة، وعند الاستيراد يتحقق النظام من التوقيع والسلامة والتوافق ويرفق تقرير الفحص ثم تُطبَّق الترقية مرحلياً بعد موافقة شخصين.

هل يحتاج أي جزء من BareStax إلى اتصال بالإنترنت أثناء التشغيل؟

لا يحتاج أي مسار تشغيلي في المنتج إلى اتصال بالإنترنت، ولا يرسل النظام بيانات إلى الخارج ولا يتصل بأي خادم بعيد. تعمل وحدة التحكم الرسومية وبوابة الباحثين وأدلة التشغيل والترخيص والعامل الثاني TOTP محلياً بالكامل، وتثبّت العُقَد حزمها من المستودع المحلي داخل العنقود.

ما مزوّدو الهوية وطرق المصادقة التي يدعمها النظام؟

ترتبط المصادقة بأدلة LDAP وActive Directory ومزوّدي OIDC وSAML إلى جانب الحسابات المحلية عند الحاجة. ويعمل العامل الثاني المدمج TOTP دون إنترنت ويُطلَب مجدداً للعمليات الحرجة ضمن نموذج صلاحيات من ستة أدوار مفصّل في صفحة الأمن.

كيف يضمن النظام موثوقية صور الحاويات على عُقَد الحساب؟

تنفَّذ المهام بحاويات Apptainer للقراءة فقط دون Docker. تمر كل صورة بسجل OCI المدمج للفحص الأمني والترقية بموافقة شخصين والتوقيع بمفتاح العنقود (مع دعم سجل المؤسسة وتوقيعها المقابل)، ولا تسمح عُقَد الحساب بتشغيل أي حاوية غير موقّعة.

الجوانب التجارية

ما سياسة دعم الإصدارات والتصحيحات الأمنية؟

يُدعَم كل خط إصدار فرعي لمدة 24 شهراً من تاريخ إطلاقه العام الأول، وتصل التصحيحات الأمنية على ذلك الخط طوال فترة الدعم. وتُحدَّد مستويات الدعم الفني وأزمنة الاستجابة والحل حسب درجة الأهمية ضمن العقد المبرم مع المؤسسة.

كيف يعمل الترخيص في بيئة معزولة؟

يعمل الترخيص محلياً دون الحاجة إلى الاتصال بأي خادم تراخيص خارجي. وللحصول على التسعير يرجى التواصل مع فريقنا.

ما اللغات المتاحة في واجهة المنتج وأدلة التشغيل؟

تتوفّر واجهة المنتج، بما يشمل وحدة تحكم المشغّل وبوابة الباحثين ورسائل سطر الأوامر وبطاقات الأخطاء المرمّزة وأدلة التشغيل المحلية، باللغة الإنجليزية فقط. ويتوفّر الموقع الإلكتروني باللغتين الإنجليزية والعربية.