All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
15 days
to the Big Data Europe CFP

VOL. I · NO. 312 SUNDAY, NOVEMBER 8, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ GATEWAY API
Envoy Gateway 1.10 encrypts OAuth2 cookies with AES-256-GCM by default P.2

◆ SUPPLY CHAIN
Ten hijacked npm packages run their loader on import, not on install P.2

◆ AI SECURITY
AWS Continuum goes GA, at about $20 per validated finding in AWS's own example P.2

AI ON KUBERNETES

Google gives gVisor and Agent Substrate to the CNCF Sandbox

Announced November 5 with OpenRL. Substrate 1.0 claims agent resume in under 500 ms at 10x container density; the figures are Google's own.

COMPILED FROM GOOGLE CLOUD BLOG AND GOOGLE OPEN SOURCE BLOG, NOVEMBER 5; THE NEW STACK, NOVEMBER 6

Google is donating three projects: gVisor, the userspace kernel under GKE Sandbox and Cloud Run; Agent Substrate, now at 1.0; and OpenRL, for self-hosted RL post-training. All three are in CNCF Sandbox onboarding.

Substrate snapshots idle agents and restores them into warm Pods in under 500 ms, at over 500 activations a second, isolated by gVisor or Cloud Hypervisor microVMs. It has 100+ contributors and powers kagent.

gVisor users include Anthropic, OpenAI and Modal; Ant Group, Modal and Tines will join as maintainers, and Google hopes neutral governance gets its I/O kernel patches upstream. What to do: try

Continued on page 2

AGENT SUBSTRATE, BY GOOGLE'S COUNT

95	AGENT IDLE TIME, % (UP TO)
20	SERVERLESS WAKE-UP, S (OVER)
10	DENSITY VS CONTAINERS, X
8	YEARS SINCE GVISOR OPENED

Google's figures, November 5; gVisor was open sourced in 2018.

AI DATA

pg_vectorsearch builds a 100M-vector index in 1h40, against 42 hours for HNSW

Tiger Data's alpha extension for PostgreSQL 18 puts a partitioned, compressed PRISM index on existing pgvector columns. The benchmark is the vendor's own.

COMPILED FROM INFOQ, NOVEMBER 7

PRISM replaces pgvector's graph-based HNSW with partitioning and compression. In Tiger Data's run on 100 million vectors it built in 1 hour 40 minutes on a 128 GB machine; HNSW, on 16-bit halfvec, took 42 hours on 512 GB. Recall@10 was checked against exact search with the open source Rekall tool.

It needs PostgreSQL 18, handles up to 1,968 dimensions and is created with CREATE INDEX ... USING prism. Filtered searches that combine WHERE and ORDER BY wait for general availability, and incremental rebalancing is unfinished, so busy tables may need index rebuilds.

Tiger Data will move pgvectorscale into maintenance mode. Coverage gives no licence or version number. What to do: try it on a copy of a large embedding table, not in production.

Full story → www.infoq.com/news/2026/11/postgresql-vector-search

SERVICE MESH SECURITY

Istio 1.31.4 and 1.30.8 fix nine flaws, led by an 8.2 ambient mTLS bypass

COMPILED FROM ISTIO SECURITY BULLETIN, NOVEMBER 6

Bulletin 2026-009, November 6: in ambient mode a port-level STRICT PeerAuthentication can be skipped, letting plaintext through, and a malformed debug request can crash-loop istiod (7.7). No attacks are reported. Upgrade.

Full story → istio.io/latest/news/security/istio-security-2026-009

CI/CD SECURITY

GitHub will block a risky Actions trigger by default from December 2

COMPILED FROM INFOQ, NOVEMBER 6; GITHUB CHANGELOG

The change, announced November 2, applies to pull_request_target. Lockfiles went GA on October 28: actions.lock pins direct and transitive actions to commits, and Dependabot updates it. A lock is not a review.

Full story → www.infoq.com/news/2026/11/github-actions-lockfiles-ga

SECRETS

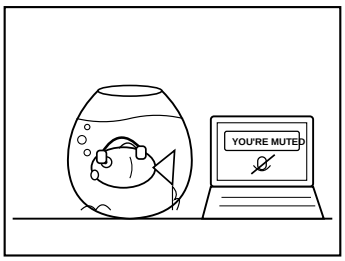
OpenBao 2.7 adds post-quantum TLS and drops file storage

COMPILED FROM INFOQ, NOVEMBER 6

The Vault fork adds ML-DSA and ML-KEM and reads on PostgreSQL standbys. Cloud auto-unseal and LDAP and Kerberos auth move to plugins: check before upgrading.

Full story → www.infoq.com/news/2026/11/vault-fork-openbao-27

CARTOON OF THE DAY



Drawing: Claude

"Sorry, I think I was on mute the whole time."

WHY IT'S FUNNY A goldfish in headphones has joined a video call and talked through the entire meeting. The laptop says it is muted, but for a fish behind glass, nobody hearing a word is the normal state of affairs.

DATES TO WATCH
Events and calls for papers

Nov 8 EVENT
CNCF Maintainer Summit, Salt Lake City

Nov 9 EVENT
Platform Engineering Day, ArgoCon, BackstageCon and FluxCon NA, Salt Lake City

Nov 9-12 EVENT
KubeCon + CloudNativeCon NA, Salt Lake City

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

core-provider 2.13.74 turns on leader election by default

November 8, 2026 — On November 6 and 7, core-provider enabled leader election, authn added public OIDC clients that sign in with PKCE, and oasgen-provider 0.54.1 fixed the apiKey breakage introduced in 0.53.0.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

core-provider 2.13.69–2.13.75 · Nov 7
- Leader election on by default from 2.13.74.

github.com/krateo-platformops/core-provider/releases

authn 0.35.5–0.36.0 · Nov 7
- Public OIDC clients sign in with PKCE.

github.com/krateo-platformops/authn/releases

oasgen-provider 0.54.0–0.54.1 · Nov 7
- Use 0.54.1 if resources use apiKey auth.

github.com/krateo-platformops/oasgen-provider/releases

installer 0.3.514–0.3.528 · Nov 7
- Pins core-provider 2.13.75, authn 0.36.0, snowplow 1.12.65.

github.com/krateo-platformops/installer/releases

frontend, portal 1.8.29–1.8.32, 1.8.94–1.8.95 · Nov 7
- Assistant renamed Agentiko; Access card added.

github.com/krateo-platformops/frontend/releases

alert-provider, observability 0.2.61–0.2.63, 3.1.42–3.1.50 · Nov 7
- No default Alerts; new JWT-in-traces alert.

github.com/krateo-platformops/alert-provider/releases

provider-, unstructured-runtime, sse-proxy 1.10.1, 1.11.0–1.12.0, 1.4.1–1.4.2 · Nov 7
- Queue-priority and saturation fixes.

github.com/krateo-platformops/unstructured-runtime/releases

Latest elsewhere: snowplow 1.12.65 (Nov 4), git-provider 0.16.0 (Nov 4), helm-render-service 0.5.0 (Sep 30); plumbing has no releases.

KRATEO AGENTIKO

Merged into main this week

Krateo Agentiko notifications could not be read this morning.

CONTINUED FROM PAGE 1 · AI ON KUBERNETES

gVisor to CNCF

github.com/agent-substrate; ATECon runs November 9 at KubeCon.

Full story → cloud.google.com/blog/products/containers-kubernetes/open-infrastructure-for-autonomous-agents-comes-to-cncf opensource.googleblog.com/2026/11/sandboxing-untrusted-ai-agents-at-scale.html

NEWS IN BRIEF

GATEWAY API

Envoy Gateway 1.10 encrypts OAuth2 cookies with AES-256-GCM by default

Out November 6 with Gateway API 1.6.2. The Lua sandbox now blocks getfenv and setfenv, and release images are signed with cosign. Endpoints-type Backends must list endpoints and zero health-check durations are rejected, so validate manifests before upgrading.

— Envoy Gateway release notes
github.com/envoyproxy/gateway/releases/tag/v1.10.0

SUPPLY CHAIN

Ten hijacked npm packages run their loader on import, not on install

Sonatype reported 12 malicious releases on November 7, including six @adminide-stack modules and cdeops 13.5.31; disabling install scripts does not help. The loader reads its server address from an Ethereum wallet. Check lockfiles and mirrors, treat hosts that ran them as compromised and rotate CI secrets.

— Daily CyberSecurity, November 7
securityonline.info/polinrider-loader-hijacked-npm-packages

AI SECURITY

AWS Continuum goes GA, at about $20 per validated finding in AWS's own example

Available in us-east-1 and us-west-2 after four months of preview, it confirms each code flaw by running an exploit in a sandbox, then proposes a patch or pull request that a person must approve. Pricing starts at $200 per million lines a month plus $10 per inference unit.

— InfoQ, November 6
www.infoq.com/news/2026/11/aws-continuum-ga

DEVELOPER TOOLS

JetBrains patches 61 flaws, led by a 9.6 admin takeover in Hub

Hub 2026.2.52556 fixes CVE-2026-123294, where an email change during login can grant admin rights; Datalore 2026.4 stops view-only users running code (9.0). YouTrack, Ktor 3.6.1 and the IDEs are also patched. No attacks are known.

— Daily CyberSecurity, November 6
securityonline.info/jetbrains-security-updates-cve-2026-123294-patched

AI INFERENCE

A CNCF post maps how vLLM, SGLang and llm-d cut inference cold starts

The DaoCloud member post sorts approaches by what they reuse: model files, compiled caches, processed weights or whole engine snapshots. Snapshot restore covers one GPU at tensor parallelism 1 today. Pod-level checkpoint and restore (KEP-5823) targets alpha in Kubernetes 1.38.

— CNCF blog, November 6
www.cncf.io/blog/2026/11/06/faster-llm-inference-startup-what-you-need-to-know

LLM SECURITY

A ChatGPT preview flaw could leak whole chats despite Lockdown Mode, now fixed

Check Point found nested iframes in HTML previews could open attacker popups; in the legacy Electron desktop app a custom GPT could send full chat logs with no click. OpenAI fixed it in September and disclosure came November 6. Keep desktop clients updated.

— Daily CyberSecurity, November 6
securityonline.info/chatgpt-lockdown-mode-bypass

PUZZLE · WORD SEARCH

Ten words from today's two pages are hidden in the grid.

FIND AMBIENT · GVISOR · ISTIO · LOCKFILE · OPENBAO · OPENRL · POSTGRES · SANDBOX · SUBSTRATE · VECTOR

P	S	R	D	U	S	B	N	B	N	S	U
H	V	N	I	R	U	L	E	O	U	P	N
P	U	E	O	B	B	A	G	I	Y	O	V
L	O	R	S	M	S	E	Y	T	T	S	V
T	P	O	U	H	T	L	S	S	N	T	E
B	E	S	T	S	R	I	A	I	E	G	C
P	N	I	U	T	A	F	N	N	I	R	T
S	B	V	M	E	T	K	D	D	B	E	O
F	A	G	A	H	E	C	B	L	M	S	R
E	O	I	D	F	H	O	O	D	A	Y	A
O	O	P	E	N	R	L	X	D	D	M	H
W	U	D	F	E	O	M	C	B	C	Y	P

Words run in every direction, also backwards.

SOLUTION

