All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
3 days
to the CN AI + Inference Day CFP

VOL. I · NO. 289 FRIDAY, OCTOBER 16, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ AI ON THE DESKTOP
Nvidia fits a 74B agent model into 24GB, at two bits a weight P.2

◆ CLOUD NATIVE SECURITY
A hostile server can free curl's upload out from under it P.2

◆ NETWORKING
Cilium was garbage-collecting conntrack entries the datapath had just reopened P.2

SUPPLY CHAIN

GhostAction hit 30,000 repositories in one afternoon

GitGuardian counted the October 8 burst on October 13: about 1,900 compromised accounts and 3,174 secrets on the shopping list.

COMPILED FROM GITGUARDIAN, REPORTED BY THE NEW STACK AND THE HACKER NEWS

About 30,000 repositories across roughly 3,000 users and organisations were targeted, a reach GitGuardian attributes to compromising the accounts of about 1,900 GitHub users. The largest batch, 29,431 commits tagged "new", started at 14:07 on October 8.

The injected workflow reads the repository's history for ${{ secrets.NAME }} references, copies those names into a new file, and POSTs the values in clear HTTP to 193.32.204.199. GitHub began blocking it on October 9.

Rotating secrets is not the whole job: the credential used to push the workflow "must be found and revoked too, or someone else will use it again".

Full story → blog.gitguardian.com/ghostaction-github-actions-supply-chain-attack-returns thenewstack.io/ghostaction-github-actions-attack

THE SEPTEMBER WAVE, IN FULL

772 PUBLIC REPOSITORIES HIT

446 SSH AND DEPLOY KEYS LISTED

373 ACCOUNTS AND ORGS AFFECTED

124 REPOSITORIES CLEANED BY OCT 5

The earlier GhostAction wave, Aug 31 to Sep 30, the one with a full post-mortem. Azure credentials came second at 218 references. Source: GitGuardian.

NEW LLM RELEASES

Meta opens 816B weights, and keeps a revenue clause on the API resellers

Muse Spark Open landed on Hugging Face on October 15. Agentic benchmarks lead the table; the general intelligence score does not.

COMPILED FROM HUGGING FACE MODEL CARD, META SUPERINTELLIGENCE LABS; THE NEW STACK

816B total parameters with 42B active, a mixture-of-experts transformer with a perception encoder, 256 experts with eight per token, and 1M tokens of context. The card asks for about 2 TB of VRAM in BF16, at least 700 GB in NVFP4.

Meta's table puts it at 39 on the Artificial Analysis Intelligence Index, behind GLM 5.3 at 45 and Kimi K3 at 44, but ahead on agentic work: 61.8 on JobBench, 89.2 on MCP-Atlas. The licence is not an OSI one, and API resellers above $20 million of gross revenue sign a separate agreement with Meta.

Full story → huggingface.co/meta-models/Muse-Spark-Open-816B-A42B thenewstack.io/meta-muse-spark-open

CLOUD NATIVE SECURITY

Capitalise the HTTP/2 method and Istio's AuthorizationPolicy stops matching

Istio 1.31.2, 1.30.6 and 1.29.9 shipped late on October 15. Four advisories, two of them in Envoy.

COMPILED FROM ISTIO.IO RELEASE ANNOUNCEMENTS

GHSA-w44g-8m76-8gc5, CVSS 7.4: changing the case of an HTTP/2 method bypasses AuthorizationPolicy method rules, so a rule written for GET never fires. GHSA-7p2q-4xvg-vxc6, 7.7: istiod crashes in ambient

Continued on page 2

AI AND HPC ON KUBERNETES

A spoofed annotation let a Pod walk past its ClusterQueue, and the fix is off by default

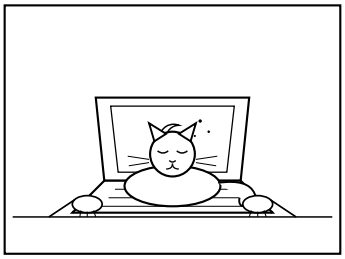
Kueue 0.20.2 and 0.19.9, October 15. Patching alone does not close this one.

COMPILED FROM GITHUB.COM/KUBERNETES-SIGS/KUEUE

A Pod could bypass ClusterQueue quota by spoofing another role's role-hash annotation. The fix sits behind the alpha PodIntegrationVerifyRoleRequests gate, disabled by default, so operators have to turn it on. A DRA requeue path that could over- or under-admit is fixed too.

Full story → github.com/kubernetes-sigs/kueue/releases/tag/v0.20.2

CARTOON OF THE DAY



Drawing: Claude

Remote work.

WHY IT'S FUNNY The cat has taken the keyboard, so the human types around it with a hand on either side. The laptop, getting nothing from the middle of the keyboard, has decided nobody is there and gone to sleep. Everyone in the picture is committed to the arrangement except the machine.

DATES TO WATCH

Events and calls for papers

Oct 13–16 ONLINE
OpenStack and OpenInfra Project Teams Gathering, virtual, last day today

Oct 17 ONLINE
GitLab CI/CD: from Git to automated deployment, free online workshop

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

snowplow 1.12.49 stops the resolver following a redirect off the apiserver

October 16, 2026 — Two snowplow releases on October 15, pinned by the installer the same day: 1.12.48 cut a list-burst heap spike from about 1,089 MiB to 56 MiB, and 1.12.49 hardened the resolver's ServiceAccount dials.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

snowplow 1.12.49 · Oct 15

- Resolver ServiceAccount dials can no longer be redirected off the apiserver, and no longer carry a stage's impersonation or authorization headers.

github.com/krateo-platformops/snowplow/releases

snowplow 1.12.48 · Oct 15

- Concurrent readers of a stale API-stage cell now share one in-flight fill, cutting the memory spike under load.
- An upstream 404 now returns 404 instead of a JSON-decode 500.

github.com/krateo-platformops/snowplow/releases

installer 0.3.428 · Oct 15

- Pins snowplow and snowplow-crd to 1.12.49, marked a security pin; 0.3.427 carried 1.12.48 earlier the same day.

github.com/krateo-platformops/installer/releases

Latest elsewhere: frontend 1.8.5, portal 1.8.72 and core-provider 2.13.25 (Oct 14), observability 0.1.22 and sse-proxy 0.1.14 (Oct 12).

KRATEO AGENTIKO

Merged into main this week

No new Krateo Agentiko pull requests since the last issue.

CONTINUED FROM PAGE 1 · CLOUD NATIVE SECURITY

Istio case

mode when a ServiceEntry claims the address of an IP-addressed waypoint.

Full story → istio.io/latest/news/releases/1.31.x/announcing-1.31.2

OBSERVABILITY

Tempo 3.1 redacts traces from a query, and the rewrite cannot be undone

Covered October 15. vParquet5 becomes the default block format and simple metrics queries run close to twice as fast.

COMPILED FROM INFOQ, GRAFANA LABS

tempo-cli redact now takes a TraceQL query instead of a list of trace IDs, with --dry-run and a time window. Workers still on 3.0 ignore that window and delete every match in each block, silently, so get the whole cluster to 3.1 first.

Full story → www.infoq.com/news/2026/10/grafana-tempo-31

NEWS IN BRIEF

AI ON THE DESKTOP

Nvidia fits a 74B agent model into 24GB, at two bits a weight

Nemotron 3.5 Bolt 74B-A9B shipped October 15: about 9B active parameters, 256K of context, quantised to roughly 24GB, under the OpenMDW-1.1 licence. Nvidia compares its 2-bit model against three rivals run in full BF16: 50.98 against Qwen3.6's 44.38 on Terminal-Bench 2.1. No third-party results yet.

— research.nvidia.com, The New Stack
research.nvidia.com/labs/nemotron/Nemotron-3.5-Bolt-24GB

CLOUD NATIVE SECURITY

A hostile server can free curl's upload out from under it

CVE-2026-92392, CVSS 8.1, published October 15. A use-after-free in HTTP/2 uploads: curl keeps a reference to a freed transfer object when handling a stream reset frame. Versions 8.12.0 to 8.22.0 of the tool and of libcurl are affected. Fixed in 8.23.0; until then force --http1.1.

— securityonline.info, curl advisory
securityonline.info/curl-cve-2026-92392-vulnerability

NETWORKING

Cilium was garbage-collecting conntrack entries the datapath had just reopened

1.20.3, 1.19.9 and 1.18.15 all landed on October 15. The conntrack GC race that deleted entries for live connections is fixed, and the operator now rejects a CiliumNetworkPolicy whose nodeSelector would silently enforce nothing.

— github.com/cilium/cilium
github.com/cilium/cilium/releases/tag/v1.20.3

CLOUD

Amazon Neptune deserialises whatever a query user sends it, at 9.9

CVE-2026-110812, October 15. Unsafe deserialisation in the Gremlin graph-import path, from Apache TinkerPop: any principal with neptune-db query permissions can send a crafted request. Engines from 1.2.0.0 are affected; fixed in 1.4.7.1, 1.4.8.1 and 1.5.0.0. Manually pinned clusters will not pick it up.

— securityonline.info, AWS security bulletin
securityonline.info/aws-patches-critical-amazon-neptune-vulnerability

KUBECTL TIP

```
kubectl auth can-i --list
```

Every verb the current token holds *(kubernetes.io)*

CLOUD NATIVE SECURITY

Next.js ships two critical RCEs out of band, and one has no workaround

Vercel released 16.4.1 and 15.5.28 on October 14. GHSA-673q-mjm6-r5xr is remote code execution when a "use cache" function returns multiple typed arrays, rooted upstream in React, with no mitigation but the upgrade. CVE-2026-96889 is a sharp memory bug reached through SVG optimisation.

— securityonline.info, Vercel advisories
securityonline.info/nextjs-security-update-rce-october-2026

KUBECTL TIP

```
kubectl get --raw /readyz?verbose
```

Each API server readiness check, one line each *(kubernetes.io)*

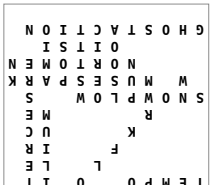
PUZZLE · WORD SEARCH

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

FIND CILIUM · GHOSTACTION · ISTIO · KUEUE · MUSESPARK · NEMOTRON · SECRETS · SNOWPLOW · TEMPO · WORKFLOW

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

Words run in every direction, also backwards.



SOLUTION