All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
2 days
to the Big Data Europe CFP

VOL. I · NO. 325 SATURDAY, NOVEMBER 21, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ SUPPLY CHAIN
Microsoft's agent-framework on PyPI shipped a stealer for 55 minutes P.2

◆ CONTAINER RUNTIME
A malformed image can crash containerd; 2.2.10, 2.3.7 and 2.4.2 fix it P.2

◆ CONTROL PLANES
Crossplane 2.5's first release candidate cuts heap from 338 to 190 MiB P.2

LLM RELEASE

Google's Gemini 4 Neon: $3 in, $15 out, close to Opus 5.5 on coding

The new top Gemini tier takes 1M tokens of context and ranks third on Artificial Analysis's index. Most other scores come from Google.

COMPILED FROM GOOGLE, VENTUREBEAT, SIMON WILLISON, NOVEMBER 18

Google released Gemini 4 Neon on November 18 at $3 per million input tokens, $0.15 cached and $15 output, with a 1M-token context. It is in the paid Gemini API, Gemini for business and the Gemini app for Pro and Ultra users. There are no open weights.

It scores 61 on the Artificial Analysis Intelligence Index, third overall. Google reports 65.2% on Terminal-Bench 4.1 against 65.8% for Opus 5.5.

VentureBeat puts the price 25% below Opus 5.5 and 50% above Sonnet 5.5. Google claims a 32% lower cost per task than Gemini 4 Carbon; Artificial Analysis says about 17%.

Full story → blog.google/innovation-and-ai/models-and-research/gemini-models/introducing-gemini-4-neon venturebeat.com/technology/google-launches-gemini-4-neon-with-opus-5-5-level-coding-performance-at-25-lower-api-token-prices

GEMINI 4 NEON SCORES

71	VALS INDEX, %
65	TERMINAL-BENCH 4.1, %
61	ARTIFICIAL ANALYSIS INDEX
56	ZAPIER AUTOMATIONBENCH, %

GITOPS

Argo CD self-heal can skip a migration hook while apps show Synced

In a five-region rollout, two Applications never ran their Sync hook, and new code ran 36 to 44 minutes against the old database schema.

COMPILED FROM CNCF BLOG (AMBASSADOR POST), NOVEMBER 20

A CNCF Ambassador post by Afzal Ansari, published November 20, describes a rollout across five regional Argo CD Applications with a migration Sync hook. Two skipped the migration yet stayed Synced and Healthy, while new code ran 36 to 44 minutes against the old schema.

He reproduced it five times out of six. When a sync window closes, a refresh reuses the recorded revision and self-heal runs a partial sync, which skips hooks and writes no history.

His fix: run the migration as a managed Job at sync-wave "-1", with a unique name per release and prune on, and test a migration that fails on purpose. The alternative is selfHeal: false on apps that migrate.

Full story → www.cncf.io/blog/2026/11/20/when-a-sync-window-closes-how-argo-cd-self-heal-skipped-the-migration-hook

SUPPLY CHAIN

Poisoned CLAUDE.md files turn AI coding tools into stealers

Bitdefender found 22 repositories aimed at 14 AI tools.

COMPILED FROM BITDEFENDER LABS, NOVEMBER 17; SECURITYONLINE, NOVEMBER 19

Rule files, a SessionStart hook in .claude/settings.json and MCP definitions lead tools such as Claude Code and Cursor to run a loader that steals GitHub, cloud and registry tokens. Check these files before opening an unknown repo.

Continued on page 2

BATCH AND HPC

Kueue 0.21 candidates list actions before upgrading

COMPILED FROM KUEUE RELEASE NOTES, GITHUB, NOVEMBER 19–20

rc.1 (November 20) rejects LeaderWorkerSets with groupIdentity: Hash and moves priority boosts to spec.priorityBoost. DRA prioritized lists are on by default: disable KueueDRAIntegration alone and Kueue will not start.

Full story → github.com/kubernetes-sigs/kueue/releases/tag/v0.21.0-rc.1

CI/CD SECURITY

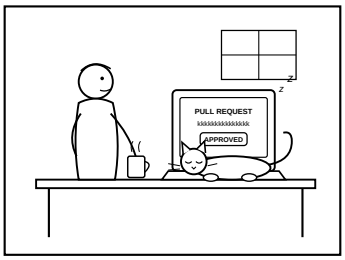
GitLab 19.6.1 patches Ruby2Shell in bundled Ruby

COMPILED FROM SECURITYONLINE, NOVEMBER 20

CVE-2026-132825 is a heap write bug in Ruby, rated 7.4 by MITRE and Critical by Ruby. Self-managed GitLab needs 19.6.1, 19.5.8 or 19.4.10; no attacks are known.

Full story → securityonline.info/gitlab-ruby2shell-vulnerability-cve-2026-132825

CARTOON OF THE DAY



Drawing: Claude

"Good news: the cat approved my pull request."

WHY IT'S FUNNY Anyone who works from home knows a cat will sooner or later lie down on a warm keyboard. This one typed a row of k's and hit the approve button, which says less about the cat than about how the review process was set up.

DATES TO WATCH
Events and calls for papers

Nov 23 CFP
Big Data Europe (Vilnius, Nov 27): talks due

Nov 24 CFP
eBPF Summit 2027: Security Edition (online, Jan 27): talks due

Nov 27 EVENT
Big Data Europe, Vilnius

Nov 28 EVENT
KCD Hangzhou

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

Krateo portal tracks token spend per agent

November 21, 2026 — From November 18 to 20, the portal added token spend per agent, user and group, and core-provider made management policies gate install and upgrade.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

portal 1.8.137–1.8.140 · Nov 18–20

- Token usage spend per agent, user and group; new dashboards.

github.com/krateo-platformops/portal/releases

core-provider 2.13.112–2.13.116 · Nov 18–19

- Management policy now gates install and upgrade; refuses to start without its CRDs.

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

installer 0.3.683–0.3.691 · Nov 18–20

- Adds controller pool support for CompositionDefinitions.

github.com/krateo-platformops/installer/releases

unstructured-, provider-runtime 1.28.0–1.29.0, 1.20.1 · Nov 18

- Observe-only objects are no longer created or updated.

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

oasgen-provider, frontend 0.84.0, 1.8.49–1.8.51 · Nov 18–19

- Chart no longer silently pins one replica; live agent steps.

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

Latest elsewhere: snowplow 1.12.74 (Nov 18), observability 3.1.109 (Nov 17), authn 0.53.0 (Nov 17), alert-provider 0.2.85 (Nov 15), helm-render-service 0.5.0 (Sep 30).

KRATEO AGENTIKO

Merged into main this week

Krateo Agentiko notifications could not be read this morning.

CONTINUED FROM PAGE 1 · SUPPLY CHAIN

Agent malware

Full story → www.bitdefender.com/en-us/blog/labs/how-ai-agents-become-new-targets-in-github-malware-campaign securityonline.info/github-ai-agent-malware-coding-assistants

NEWS IN BRIEF

SUPPLY CHAIN

Microsoft's agent-framework on PyPI shipped a stealer for 55 minutes

Versions 1.26.1 and 1.26.2, uploaded November 17, took cloud keys and GitHub Actions tokens. Pin 1.26.0, purge both from caches and images, and rotate secrets; Wiz warns that a plain pip uninstall re-runs the payload.

— SecurityOnline, November 18
securityonline.info/agent-framework-pypi-attack

CONTAINER RUNTIME

A malformed image can crash containerd; 2.2.10, 2.3.7 and 2.4.2 fix it

CVE-2026-95839 (CVSS 7.1) panics containerd on a crafted image digest, and kubelet retries keep crashing it. Disclosed October 13, listed by GitHub November 19. Upgrade, or allow only trusted registries.

— GitHub Advisory Database, November 19
github.com/advisories/GHSA-vwhp-8p66-mq4f

HELM TIP

`helm get hooks my-release`

Print the hooks of a release *(helm.sh)*

MCP SECURITY

k8s-mcp-server ran cluster tools for anyone who could reach it

Before 1.1.0 its default HTTP transport had no authentication, so anyone could call its create, delete and Helm tools (CVE-2026-130007, CVSS 7.9). Upgrade, or bind it to loopback.

— GitHub Advisory Database, November 19
github.com/advisories/GHSA-m932-63jc-4jqq

GITOPS

Argo CD 3.6.2, 3.5.8 and 3.4.14 patch a regex library CVE

Released November 18, all three fix CVE-2026-77299 in dlclark/regexp2 and stop AppProject deny rules vetoing allowed destinations. No manual steps.

— Argo CD release notes, GitHub, November 18
github.com/argoproj/argo-cd/releases/tag/v3.6.2

GITOPS

Flux 2.10.1 applies credential annotation changes without a restart

Out November 20, it picks up ServiceAccount auth annotation changes on the next reconcile and restores registry auth behind private token services.

— Flux release notes, GitHub, November 20
github.com/fluxcd/flux2/releases/tag/v2.10.1

NUMBER OF THE DAY

44 minutes new code ran on old schema *(CNCF blog)*

CONTROL PLANES

Crossplane 2.5's first release candidate cuts heap from 338 to 190 MiB

On 791 CRDs, rc.1 (November 18) stops caching CRD schemas. It reserves status.crossplane on modern XRs: move any XRD fields there first. Not for production.

— Crossplane release notes, GitHub, November 18
github.com/crossplane/crossplane/releases/tag/v2.5.0-rc.1

DEVELOPER TOOLS

Git LFS 3.8.1 stops crafted .lfsconfig files from running commands

CVE-2026-105803 (CVSS 8.6) lets a malicious repository run a command on fetch. GitHub listed it November 20; upgrade, as the 2.x line gets no fix.

— GitHub Advisory Database, November 20
github.com/advisories/GHSA-x72p-hmqp-46hw

POLICY

Kyverno 1.19.2 cuts CEL engine time from 4.91 ms to 0.16 ms

Converting each object once per request cut allocations from 37,055 to 2,718 in a 16-policy benchmark, says a Nirmata engineer's November 18 member post.

— CNCF blog (member post), November 18
www.cncf.io/blog/2026/11/18/optimizing-kubernetes-admission-control-where-kyvernos-cel-admission-cost-actually-goes

KUBECTL TIP

`kubectl auth whoami`

Show who your requests run as *(kubernetes.io)*

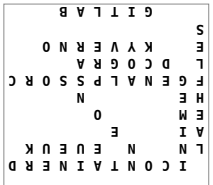
PUZZLE · WORD SEARCH

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

FIND ARGOCD · CONTAINERD · CROSSPLANE · FLUX · GEMINI · GITLAB · KUEUE · KYVERNO · NEON · SELFHEAL

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

Words run in every direction, also backwards.



SOLUTION