



KubeCon



CloudNativeCon

Europe 2022

WELCOME TO VALENCIA





KubeCon



CloudNativeCon

Europe 2022

Releasing Kubernetes Less Often and More Secure

SIG Release Update

Adolfo García Veytia (Chainguard)

Carlos Panato (Chainguard)

Jeremy Rickard (Microsoft)

Sascha Grunert (Red Hat)

Stephen Augustus (Cisco)





KubeCon



CloudNativeCon

Europe 2022

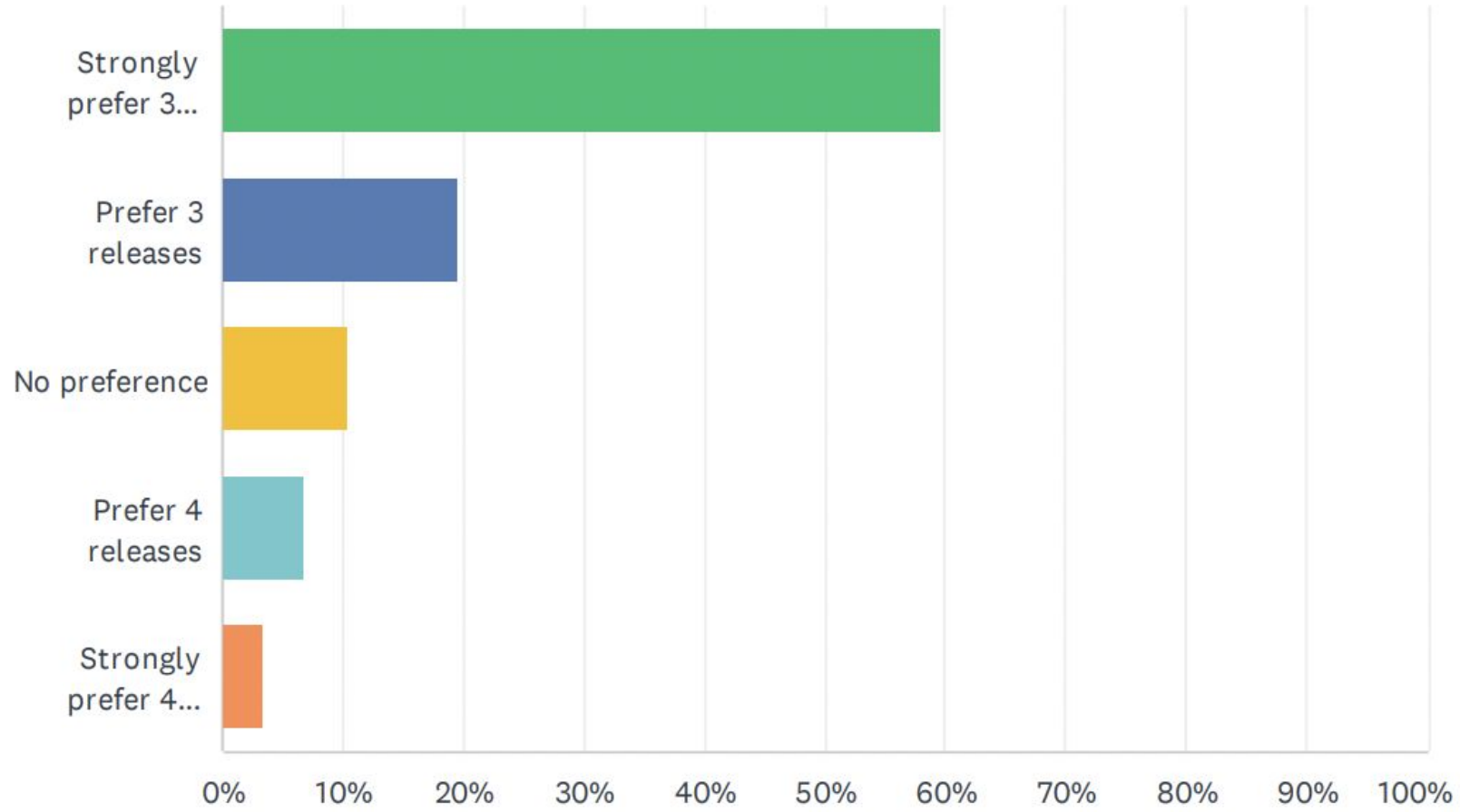


Contents of this talk

1. Changes to the Kubernetes Release Cycle
2. Release Engineering updates
 - Automatic Branch fast forward
 - Container Image signing
 - Software Bill of Materials (SBOM) security enhancements
 - Supply chain Levels for Software Artifacts (SLSA) improvements
 - GitHub Kubernetes/kubernetes main repository branch rename
3. Maintaining a Roadmap and Vision for our future goals
4. Shoutouts to our community members

Changes to the Kubernetes Release Cycle

Answered: 87 Skipped: 0



Automatic Branch Fast Forward in Code Freeze

Goal:

Continuous automated fast forwarding of the new release branch during code freeze to even it with `kubernetes/kubernetes:master`

Plan ([issue 2386](#))

- Tested in ***mock*** mode during 1.24 release cycle
- Will run in production as ***nomock*** at the end of the 1.25 release cycle



[Testgrid](#)

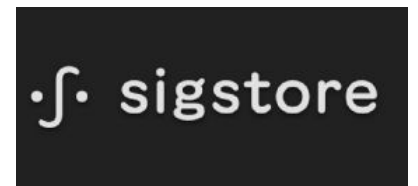


[Documentation](#)

Image Signing

Signing MVP is ready! 🎉🎉

- Initial Implementation of [KEP-3031](#)
- 55+ PRs and issues across 9 repositories and 2 orgs (Kubernetes + sigstore)
- Team of 10 contributors across 3 SIGs + support from the sigstore community 💖💖



Challenges:

- Infrastructure
- Impersonation
- Promotion
- Adapting to current processes

Coming Up:

Sign SBOM + Sign Provenance = SLSA 2!

Image Signing in the News!



KubeCon



CloudNativeCon

Europe 2022

THE NEW STACK Podcasts Events Ebooks Newsletter Sponsorship

Architecture Development Operations

CONTAINERS / KUBERNETES / SECURITY

Kubernetes Adopts Sigstore for Supply Chain Security

6 May 2022 10:39am, by Steven J. Vaughan-Nichols

ZDNet

Trending Innovation Security Business Finance Education Home & Office More

Join / Log In

MUST READ: This phishing attack delivers three forms of malware. And they all want to steal your data

Kubernetes taps Sigstore to thwart open-source software supply chain attacks

The Kubernetes project takes a step forward in shielding users from supply chain attacks on its users.

Written by **Liam Tung**, Contributor
on May 4, 2022 | Topic: Open Source

Let's talk about how companies track your data across the internet

WATCH NOW

RELATED

White House joins OpenSSF and the Linux Foundation in securing open-source software

It's not easy getting an open-source company off the ground, Appwrite wants to help

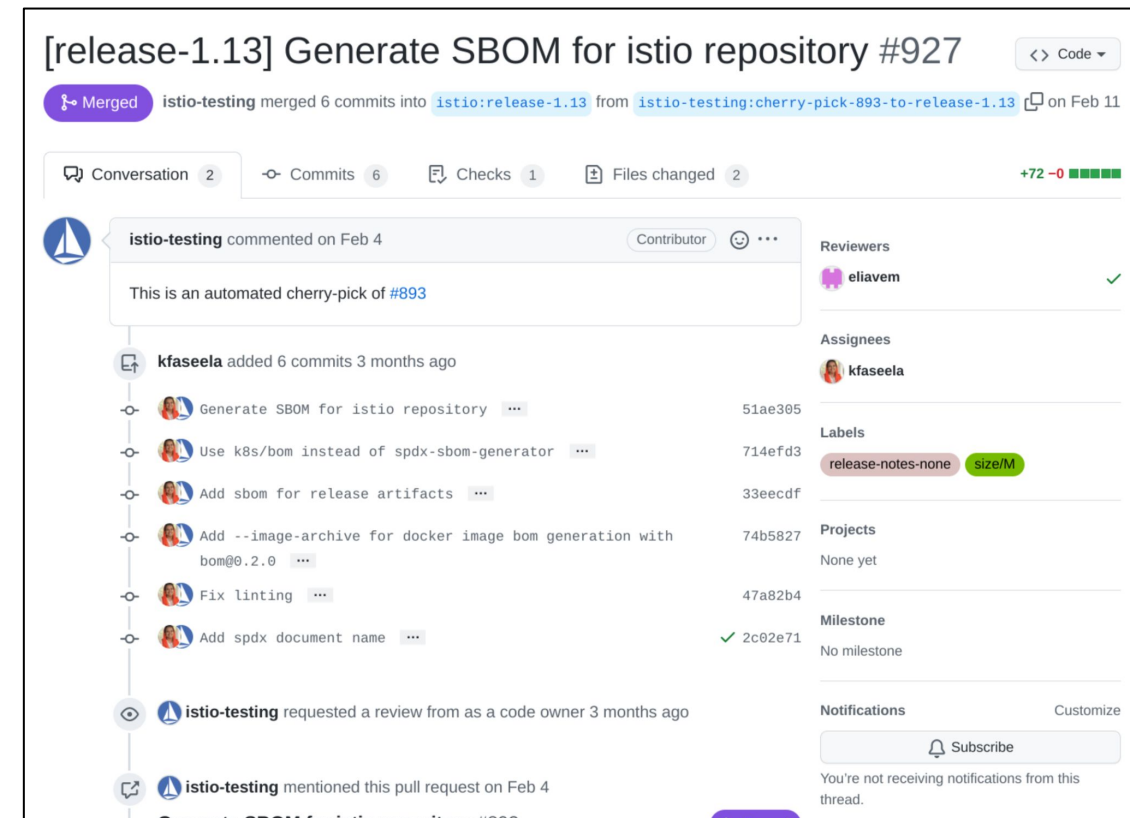
Open-source security: It's too easy to upload 'devastating' malicious packages, warns Google

NEWSLETTERS

Software Bill of Materials

Kubernetes SBOM tool

- SPDX compliant SBOMS easy, for any project
- Incubating in the Linux Foundation's Automated Compliance Tooling TAC
- Gaining traction:
 - Adopted by other projects
 - 18 Contributors



SLSA Compliance

SLSA Level 3 Compliance in the Kubernetes Release Process #3027

[Edit](#)[New issue](#)

Open

puerco opened this issue on Oct 30, 2021 · 7 comments



puerco commented on Oct 30, 2021 • edited



Enhancement Description

- One-line enhancement description (can be used as a release note): SLSA compliance for the Kubernetes release process
- Kubernetes Enhancement Proposal:
- Discussion Link:
- Primary contact (assignee): @puerco
- Responsible SIGs: SIG Release
- Enhancement target (which branch/milestone):
 - SLSA Level 1: 1.23
 - SLSA Level 2: 1.24
 - SLSA Level 3: 1.25

/sig release

/cc @kubernetes/sig-release-leads @kubernetes/release-managers

Assignees



No one—assign yourself

Labels



area/release-eng

sig/release

Projects



None yet

Milestone



No milestone

Development



[Create a branch](#)

for this issue or link a pull request.

SLSA Compliance

Supply chain Levels for Software Artifacts

Pushing towards **SLSA 2** compliance!

Done Parts:

- Provenance attestations available which
 - Identifies the builder
 - Identifies the build point
 - Identifies the build instructions

Missing Parts:

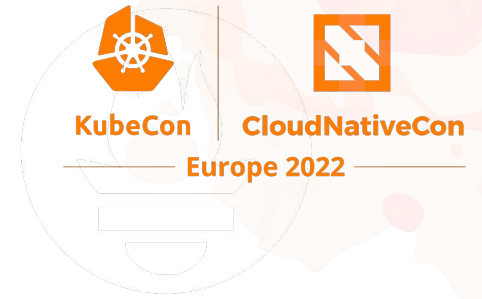
- Provenance integrity **MUST** be verifiable (signed)
- Provenance should be generated from the build system



Branch Rename (master → main)

- KEP-2853 <https://github.com/kubernetes/enhancements/pull/3053>
- Survey is out: <https://www.surveymonkey.com/r/k8s-branch-rename>
 - Fill that if you/your company uses upstream for downstreams work
 - Survey closes end of May
- Results so far says that require small changes in CI and looks like the schedule is fine
- Plan is to implement the change after code freeze for 1.25

Maintaining a Roadmap and Vision for our future goals



PromCon
North America 2021

<https://github.com/kubernetes/sig-release/blob/master/roadmap.md>

Thank you!



KubeCon



CloudNativeCon

Europe 2022

rinkiyakedad
liggitt jimangel vinayakankugoyal
wilsonehusin mkorbi onlydole
uablrek jameslaverack pmmalinov annajung
parulsahoo xmudrii tylerferrara
jrsapi ameukam sftim justaugustus dims
saschagrunert puerco leonardpahlke
lp-francois damans cpanato listx pluies
aurasinis cici rikatz pohly
bentheelder palnabarun amwat neolit
jlbutler sttts reylejano nikhita
verolop jeremyrickard spiffxp
gracenng mnaser

Where to find us

- Chairs
 - [Stephen Augustus](#), Cisco
 - [Sascha Grunert](#), Red Hat
- Tech Leads
 - [Adolfo García Veytia](#) , Chainguard
 - [Carlos Panato](#), Chainguard
 - [Jeremy Rickard](#), Microsoft
- Home page: <https://git.k8s.io/community/sig-release/README.md>
- Slack channel: <https://kubernetes.slack.com/messages/sig-release>
- List: <https://groups.google.com/forum/#!forum/kubernetes-sig-release>

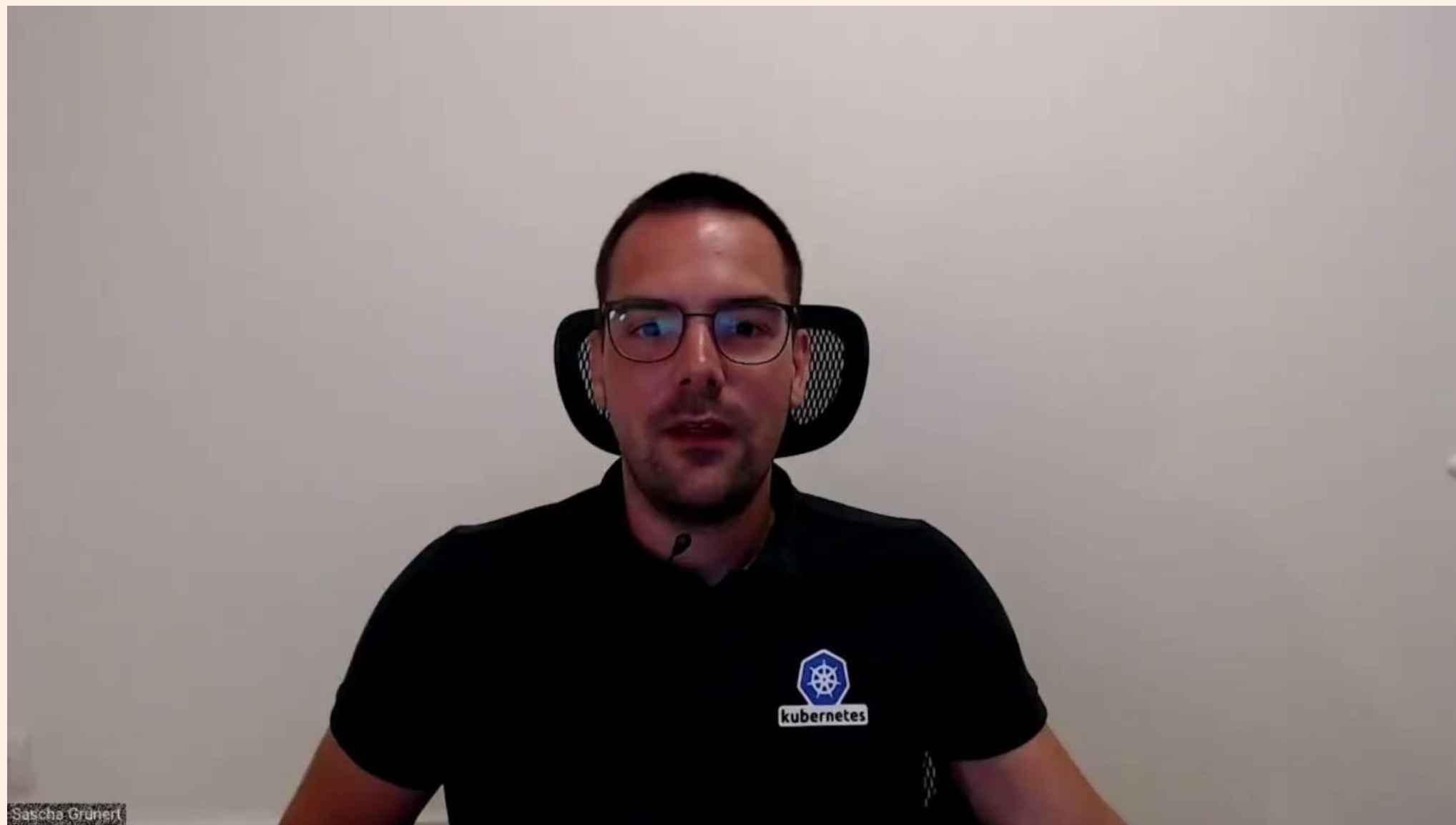


KubeCon



CloudNativeCon

Europe 2022



Sascha Grüner



Releasing Kubernetes Less Often and More Secure

SIG Release Update

Thank you for listening to our talk!



KubeCon



CloudNativeCon

Europe 2022

