
HELM
TiKV
KubeCon
CloudNativeCon
Europe 2023

KubeCon | CloudNativeCon

Europe 2023

How SIG-Release Makes Kubernetes Releases Even More Stable and Secure

Veronica Lopez, PlanetScale
Marko Mudrinić, Kubermatic GmbH

Agenda

- SIG Release Introduction
- Release Team
- Supply Chain Security
- Registry Changes
- Packages

Welcome to SIG Release!

- SIG Release is a group responsible for ensuring quality Kubernetes releases.
- This includes managing the release process of Kubernetes, following the progress of a release cycle, guiding contributors along the way, but also maintaining tooling need to release Kubernetes.
- SIG Release ensures that each release is stable, reliable, on time, and secure.
- We work in collaboration with other SIGs.

Kubernetes 1.27

- Kubernetes 1.27: Chill Vibes
- First release of 2023!
- 60 enhancements
  - Alpha: 18 enhancements
  - Beta: 29 enhancements
  - Stable: 13 enhancements

Who’s The Release Team?

- Release Team is a subteam under the SIG Release responsible for ongoing release cycle
- This includes roles such as Enhancements, Release Notes, Communications, Bug Triage, CI Signal, and Docs
- One of the main responsibilities include ensuring all changes land on time and making sure that the project stays stable through the release cycle, but especially before the release

How to Join The Release Team?

- We have a shadow application survey that's usually going up before the release cycle begins
- We will have the shadow application survey for the 1.28 release cycle after KubeCon, so take a look if you're interested!
- We recommend taking the following steps to prepare:
  - Join the Dev and SIG Release mailing lists
  - Check out the 1.28 release cycle calendar
  - Check out the Release Team Role Handbooks

How to Join The Release Team?

The 1.28 Release Cycle Overview

- **Shadow Application Closes: Tuesday 2nd May 2023 (23:59 UTC)**
- **Release Team Shadow Notifications send out latest until: 9th May 2023**
- Start date: 15th May 2023
- Planned release date: 15th August 2023 (approximately!)
- Release Team Lead: Grace Nguyen
- Release Team Emeritus Adviser: Leo Pahlke

Supply Chain Security

- We’re now SLSA 1 & SLSA2 compliant!
- SLSA 3 is work in progress.
  - We’re actively working on some of the tooling that is going to help us to achieve SLSA3.
  - Follow the KEP-3027 for more information about the progress.

Supply Chain Security

- The signing efforts have graduated to beta in the Kubernetes 1.26 release
- We started signing binary artifacts from December 2022
- However, we encountered some issues with signing container images along the way
  - We learned a lot from this and we're working hard on fixing all those issues
  - What we have: refactoring promo tools, signatures, registries, rate limits

Supply Chain Security

- We didn’t encounter many problems implementing SLSA concepts, but the real issue came when we had to scale up the implementation
  - We have 30 images per each release that we publish to 40+ different registries
  - That means a lot of push, sign, and other relevant operations!
  - On that scale, it’s super easy to fall into rate limits, and other issues that are not so obvious when working on implementation

Supply Chain Security

- Some examples of the issue we encountered along the way:
  - Google Artifact Registry rate limits (50k per 10 minutes and 5k per minute)
  - Sigstore/cosign rate limits
- However, if promoter fails in the process, we can’t always recover, so it can happen that some images remain completely or partially unsigned
  - This actually happened for February and March 2023 patch releases

Supply Chain Security For Everyone

- We have many tools we're working on: BOM, tejolote, and more!
- The goal is to make those tools available and usable for everyone.
- Check out the "Secure Your Project with the SIG Release Supply Chain Kit" session from Carlos and Adolfo on Thursday at 16:30.

Registry Changes

- We introduced **registry.k8s.io** at KubeCon NA 2022 as **a new frontend for all Kubernetes images and a replacement for k8s.gcr.io**
- The idea behind this new image registry is to be able to **serve images from both GCP and AWS**, but potentially also from other providers
  - **We got $3 million in cloud credits for AWS**, so we wanted to take that opportunity and serve images from AWS as well

Registry Changes

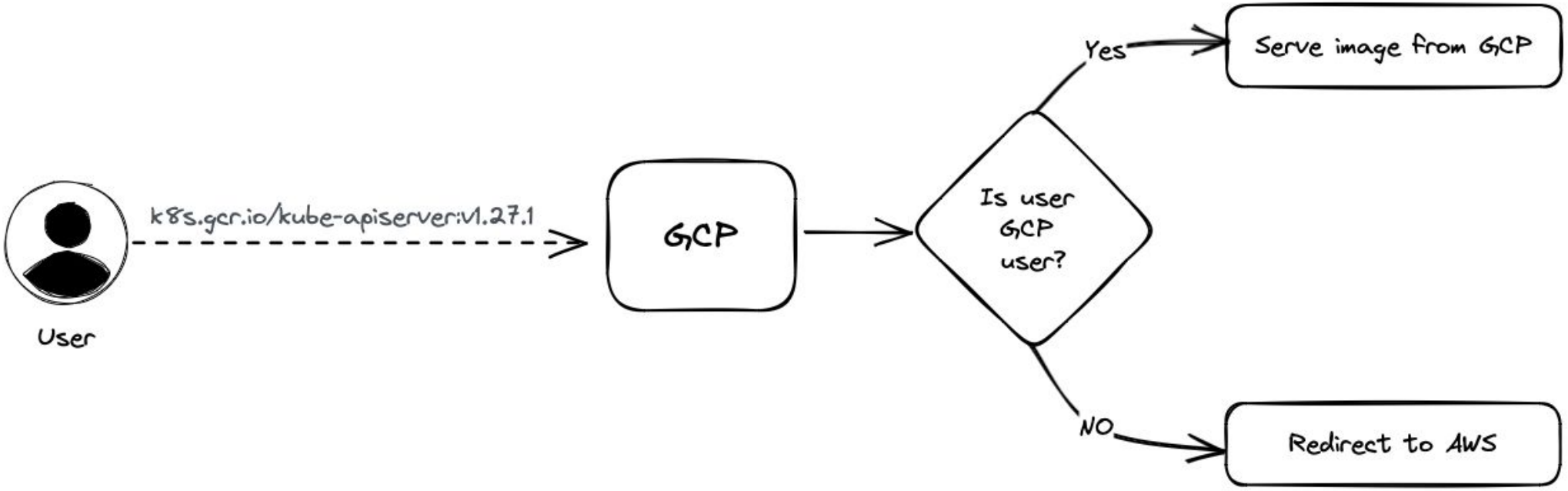
- However, just introducing the new image registry was not enough! We had to make sure that users migrate from k8s.gcr.io to registry.k8s.io.
  - That required manual interaction that we had to enforce in some way.
- **And we had to do it fast, because we were at a high risk of not having enough GCP cloud credits for 2023!**
  - We spent $600k more GCP cloud credits in 2022 than we initially got from Google for that year. We couldn’t afford that to happen in 2023.

Registry Changes

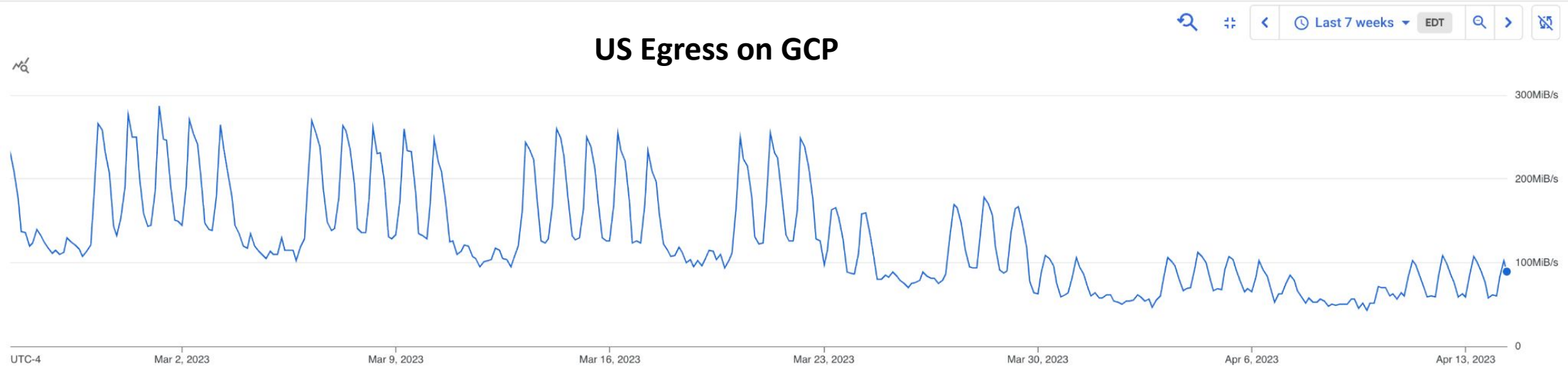
- **To make redirection go faster, we had to bend our policies**
  - Tl;dr: At least 12 months must be allowed for users to migrate away
  - While we didn’t want to remove k8s.gcr.io, we had to introduce some **backwards incompatible changes**

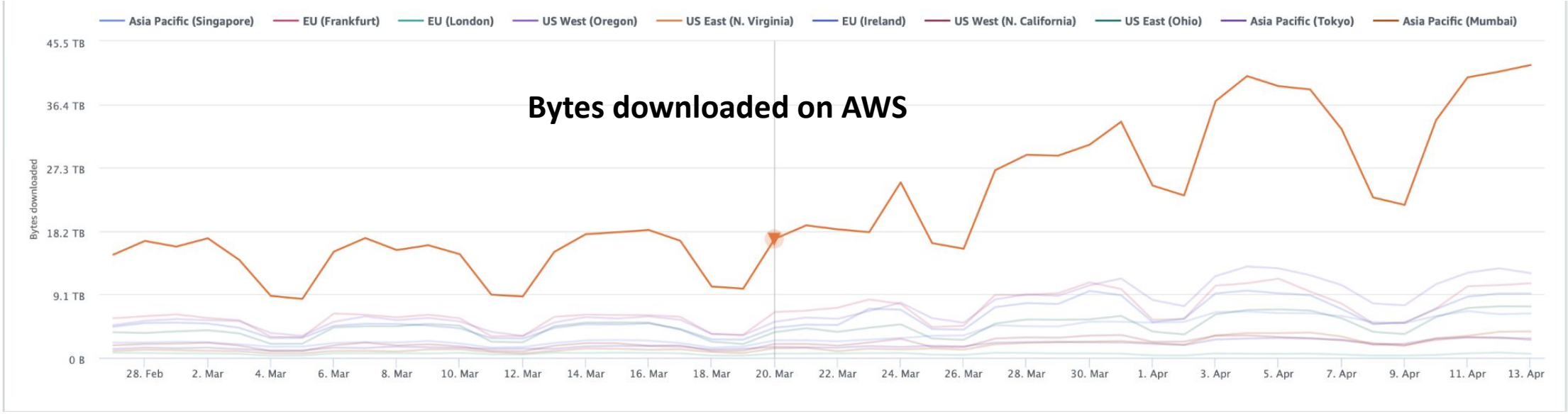
Registry Changes

- December 2022: change default image registry to registry.k8s.io in Kubernetes for all releases up to 1.22
- **20 March 2023: redirection from k8s.gcr.io to registry.k8s.io**
- 03 April 2023: freezing k8s.gcr.io



Registry Changes





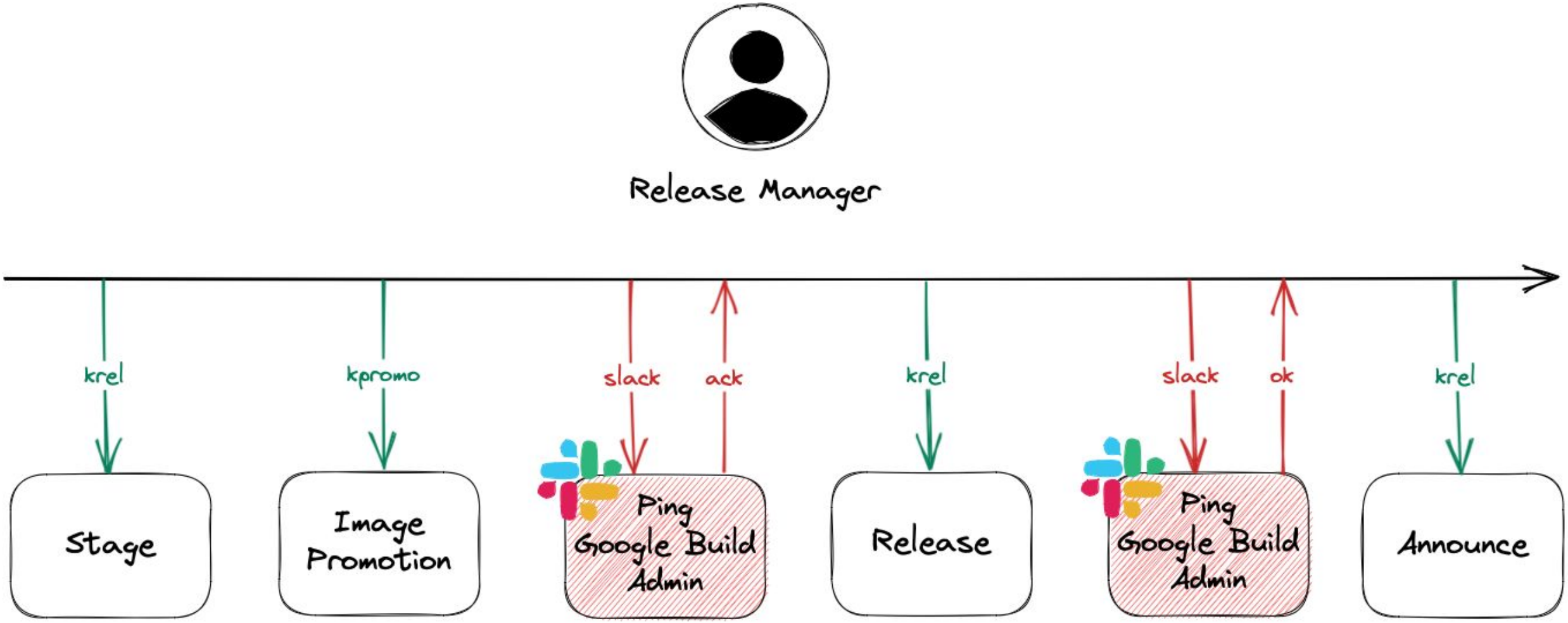
Packages

- One of the most demanded improvements is that we improve the state of Debian and RPM packages.
- **Improve stability and reliability, create packages for prereleases, and allow other subprojects to easily create and publish packages.**
- We’re trying to solve this as part of KEP-1731.

Packages - The Current Situation

- Initially, the Kubernetes packages were built, published, and hosted by Google
- Recently, we started building packages in our own pipeline, but packages are still published and hosted by Google
- **We don’t have any access to the Google infra for packages, so we depend on Google folks to trigger the publishing process for us**

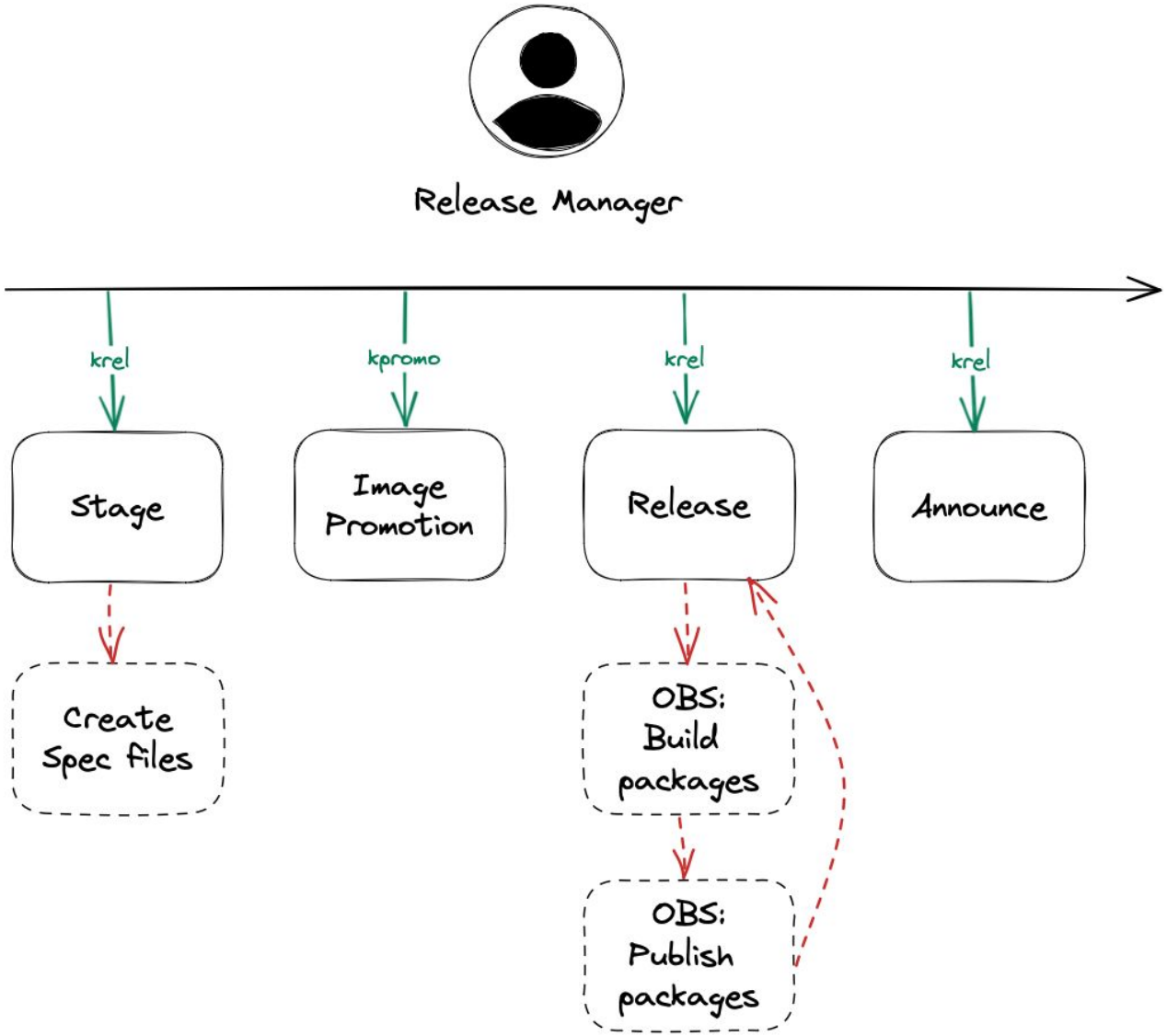
Packages - The Current Situation



Packages - Proposed Solution

- **We are being sponsored by openSUSE to use their OpenBuildService platform for building, publishing, and serving packages**
- This time, we'll have access to the platform, so that we can fully manage and publish packages on our own! 🎉
- But we need to change our release process to integrate with OpenBuildService and this requires some significant changes…

Packages - Proposed Solution



Packages - Proposed Solution

- Change Debian/RPM package spec files - **DONE**
- Change release tooling for generating spec files - **PARTIALLY DONE**
- Integrate new tooling for generating package spec files in krel - **TODO**
- Invoke OpenBuildService APIs from krel - **TODO**
- Implement tests to ensure stability and reliability of packages - **TODO**
- Sorting out permissions and access to the OpenBuildService platform - **TODO**
- Communicate, communicate, and communicate - **BLOCKED**

Packages - Proposed Solution

- The help is always very appreciated!
  - If you want to contribute to this, please reach out to SIG Release
  - For more information about the progress, follow KEP-1731 and subscribe to the SIG Release mailing list

Getting Involved with SIG Release

- If you want to get involved with SIG Release, you can always reach out to us via
  - #sig-release channel on Kubernetes Slack
  - SIG Release mailing list
  - SIG Release weekly meetings

Please scan the QR Code above
to leave feedback on this session