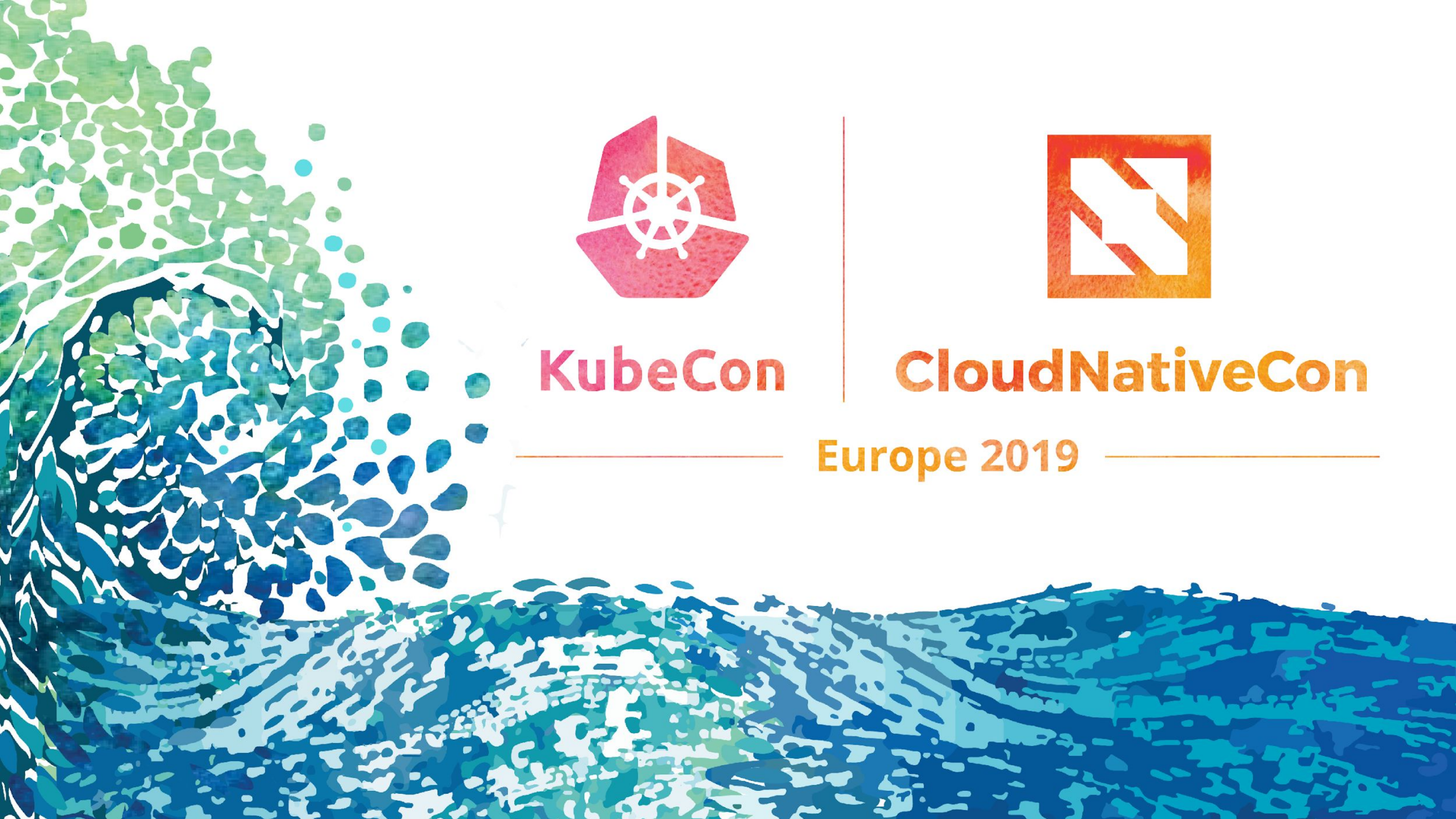


KubeCon | CloudNativeCon

Europe 2019

KubeCon | CloudNativeCon

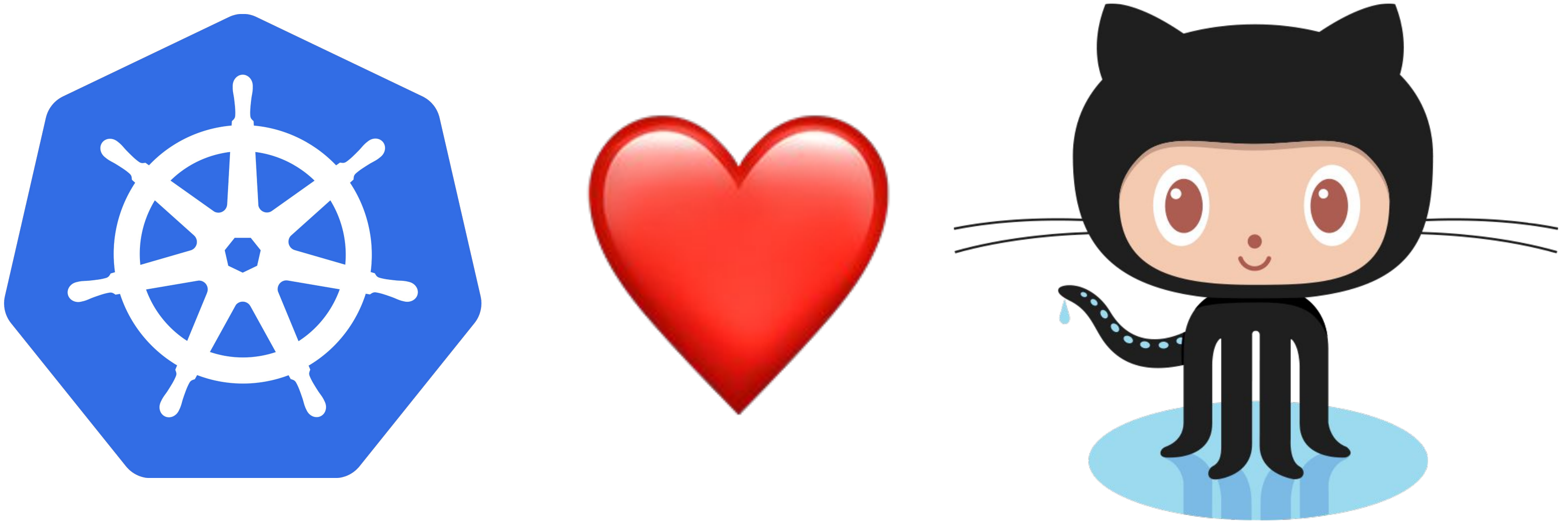
Europe 2019

Peribolos

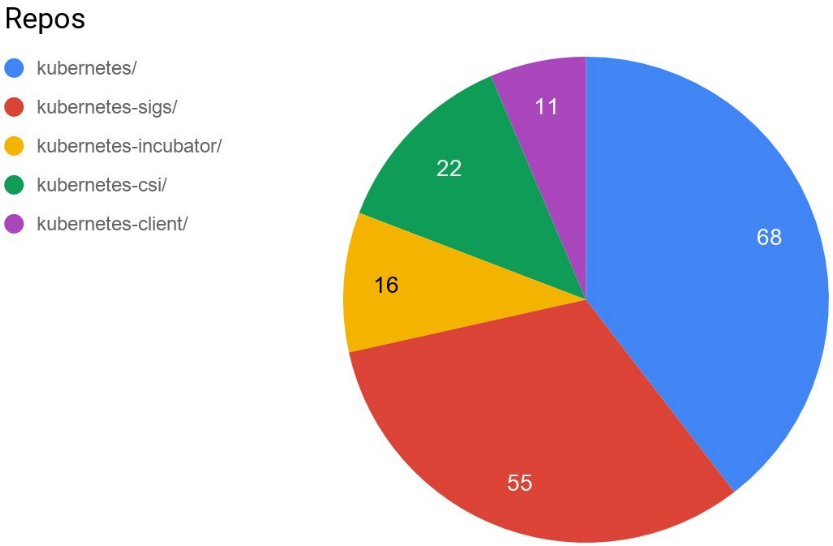
How Kubernetes uses gitops to manage GitHub communities at scale

Christoph Blecker, Red Hat
Erick Fejta, Google

Kubernetes <3 GitHub



Kubernetes GitHub footprint



As of May 2019:

- 5 primary orgs
- 172 repos
- 500+ GitHub teams
- 930+ unique members
- Over 170 new members in the first five months of this year

The Challenges and Goals

Challenges:

- Limited access levels -- many changes require “owner” privileges
- Settings spread across many different web pages
- Multi-screen processes to accomplish goals
- No visibility to changes outside of sensitive audit logs

Goals:

- Clear and simple exposure of settings
- Ability to make changes settings across all orgs
- Visibility and audit trail into changes
- Periodic reconciliation of desired state
- Delegation of privilege wherever possible
- Accomplish this in a *safe* way

Peribolos

"court enclosed by a wall, especially one surrounding a sacred area"

Dumping configuration

```
docker run gcr.io/k8s-prow/peribolos --help
# go get -u k8s.io/test-infra/prow/cmd/peribolos
# bazel build //prow/cmd/peribolos
```

Dumping configuration

```
docker run gcr.io/k8s-prow/peribolos --help
# go get -u k8s.io/test-infra/prow/cmd/peribolos
# bazel build //prow/cmd/peribolos
```

Basic design:

- First dump current org state to file
- while true; do
  - Update file to desired state
  - Reconcile desired and actual state
- Manage org metadata, teams, members (eventually repos?)

Dumping configuration

```
docker run gcr.io/k8s-prow/peribolos --help
# go get -u k8s.io/test-infra/prow/cmd/peribolos
# bazel build //prow/cmd/peribolos
```

Safe

- Problems should be funny/inconvenient, not frustrating/tragic
- Unit test config
- Separate job from presubmits
- Ensure bot, multiple admins, essential admins retain access
- Reject large deletions
- Unit testing

Dumping configuration

```
docker run gcr.io/k8s-prow/peribolos --help
# go get -u k8s.io/test-infra/prow/cmd/peribolos
# bazel build //prow/cmd/peribolos
```

Convenient

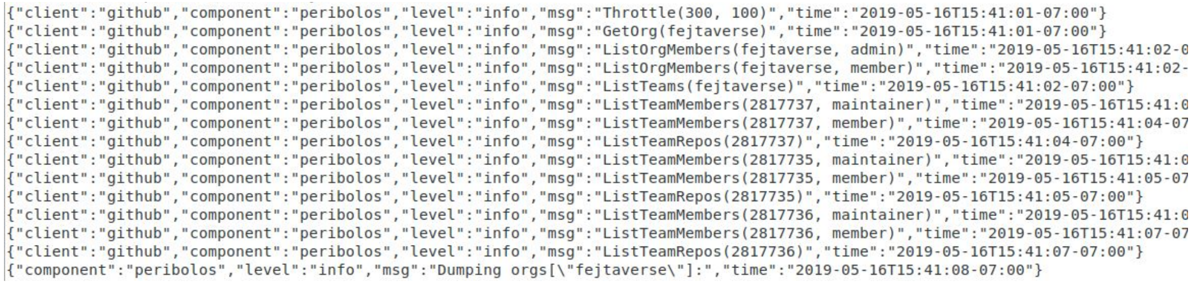
- Re-entrant
  - Fix code or config and try again
- Use config for humans
  - Unique team names
  - Skip managing uninteresting/secret metadata
- Delegate to SIGs
  - Self-service inside their own folder via OWNERS

Dumping configuration

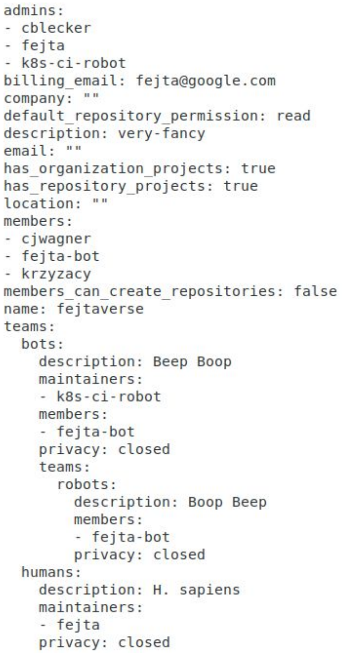
```
docker run gcr.io/k8s-prow/peribolos --help
# go get -u k8s.io/test-infra/prow/cmd/peribolos
# bazel build //prow/cmd/peribolos
```

Dumping configuration

peribolos --dump=$ORG --dump-full --github-token-path=$TOKEN > org.yaml



```
{"client":"github","component":"peribolos","level":"info","msg":"Throttle(300, 100)","time":"2019-05-16T15:41:01-07:00"}
{"client":"github","component":"peribolos","level":"info","msg":"GetOrg(fejtaverse)","time":"2019-05-16T15:41:01-07:00"}
{"client":"github","component":"peribolos","level":"info","msg":"ListOrgMembers(fejtaverse, admin)","time":"2019-05-16T15:41:02-0
{"client":"github","component":"peribolos","level":"info","msg":"ListOrgMembers(fejtaverse, member)","time":"2019-05-16T15:41:02-
{"client":"github","component":"peribolos","level":"info","msg":"ListTeams(fejtaverse)","time":"2019-05-16T15:41:02-07:00"}
{"client":"github","component":"peribolos","level":"info","msg":"ListTeamMembers(2817737, maintainer)","time":"2019-05-16T15:41:0
{"client":"github","component":"peribolos","level":"info","msg":"ListTeamMembers(2817737, member)","time":"2019-05-16T15:41:04-07
{"client":"github","component":"peribolos","level":"info","msg":"ListTeamRepos(2817737)","time":"2019-05-16T15:41:04-07:00"}
{"client":"github","component":"peribolos","level":"info","msg":"ListTeamMembers(2817735, maintainer)","time":"2019-05-16T15:41:0
{"client":"github","component":"peribolos","level":"info","msg":"ListTeamMembers(2817735, member)","time":"2019-05-16T15:41:05-07
{"client":"github","component":"peribolos","level":"info","msg":"ListTeamRepos(2817735)","time":"2019-05-16T15:41:05-07:00"}
{"client":"github","component":"peribolos","level":"info","msg":"ListTeamMembers(2817736, maintainer)","time":"2019-05-16T15:41:0
{"client":"github","component":"peribolos","level":"info","msg":"ListTeamMembers(2817736, member)","time":"2019-05-16T15:41:07-07
{"client":"github","component":"peribolos","level":"info","msg":"ListTeamRepos(2817736)","time":"2019-05-16T15:41:07-07:00"}
{"component":"peribolos","level":"info","msg":"Dumping orgs[\"fejtaverse\"]:","time":"2019-05-16T15:41:08-07:00"}
```



```
admins:
- cblecker
- fejta
- k8s-ci-robot
billing_email: fejta@google.com
company: ""
default_repository_permission: read
description: very-fancy
email: ""
has_organization_projects: true
has_repository_projects: true
location: ""
members:
- cjwagner
- fejta-bot
- krzyzacy
members_can_create_repositories: false
name: fejtaverse
teams:
  bots:
    description: Beep Boop
    maintainers:
    - k8s-ci-robot
    members:
    - fejta-bot
    privacy: closed
    teams:
      robots:
        description: Boop Beep
        members:
        - fejta-bot
        privacy: closed
  humans:
    description: H. sapiens
    maintainers:
    - fejta
    privacy: closed
```

Declare updated config

```
vim org.yaml
```

- Edit org
  - metadata (--fix-org)
  - admins and members (--fix-org-members)
- Edit teams
  - names/metadata (--fix-teams)
  - Maintainers and members (--fix-team-members)
  - Repo permissions (--fix-team-repos)

Apply declared config

```
peribolos --config-path=org.yaml --github-token-path=$TOKEN --fix-teams # --confirm
```

- Apply current config

Apply declared config

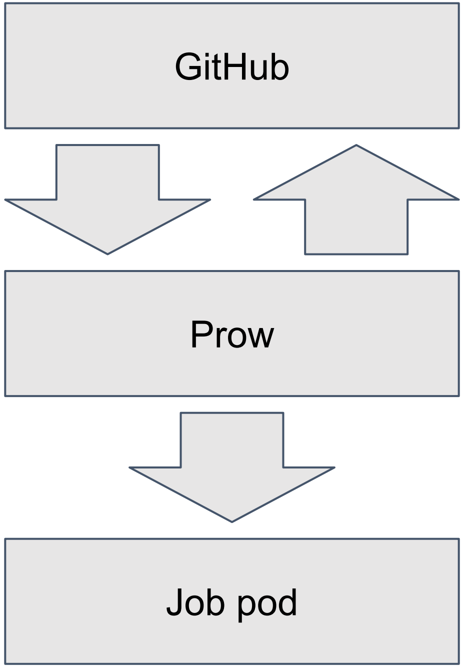
```
peribolos --config-path=org.yaml --github-token-path=$TOKEN --fix-teams # --confirm
```

- ~~Apply current config~~
- Apply current config **with gitops**

Prow - a kubernetes-centric CI/CD system from and for the kubernetes community

Github Events:

- Merge PR
- Push commit
- Left comment



GitHub

Prow

Job pod

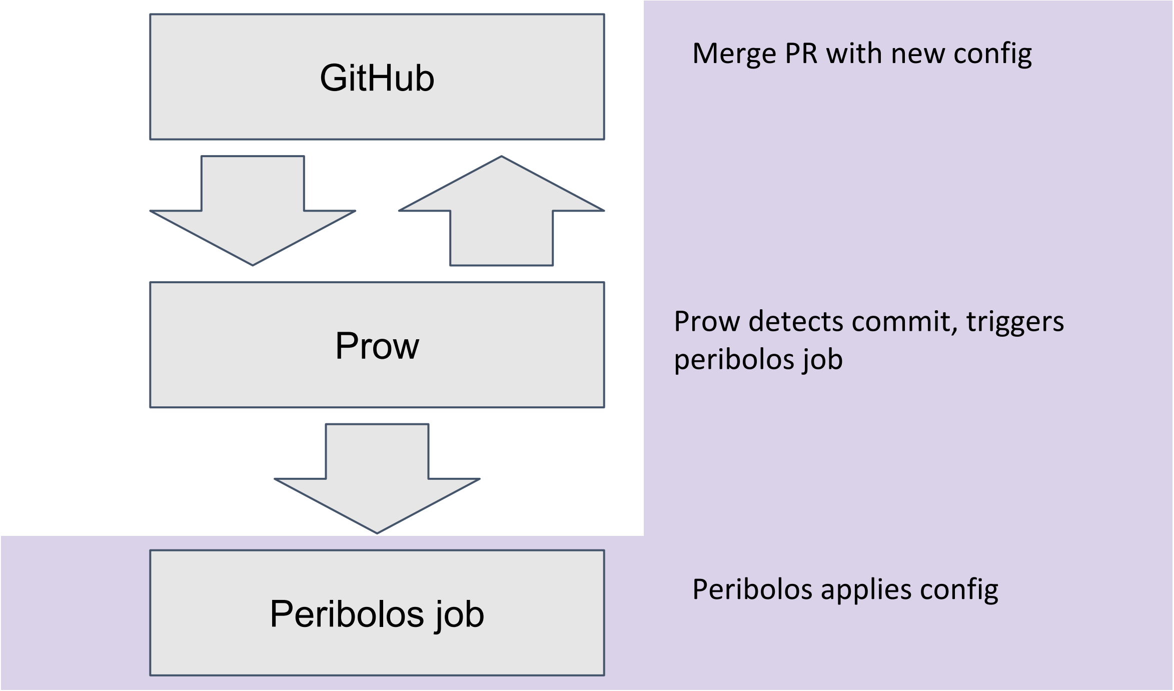
Prow Responses:

- Update status context
- Leave comment
- Change labels

Prow actions

- check out repos
- Start pod
- wait for pod
- Upload logs

Prow + peribolos

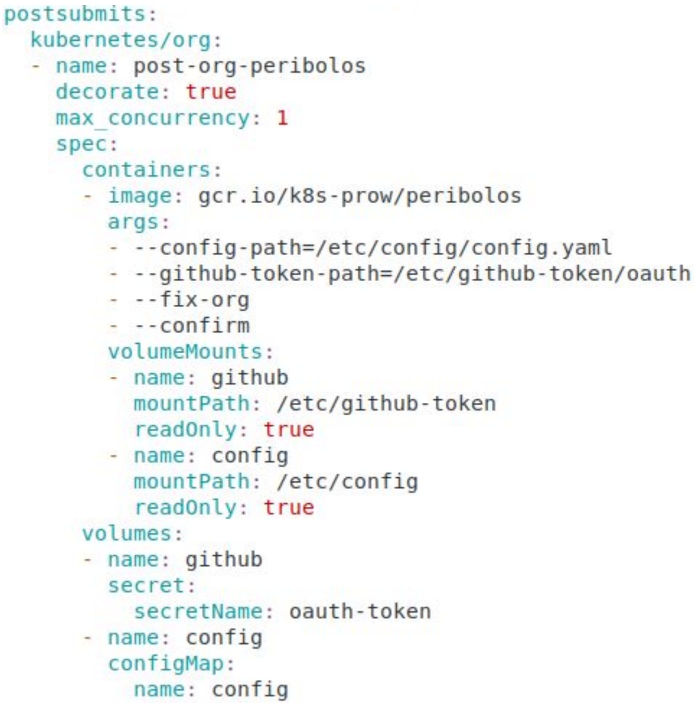


Merge PR with new config

Prow detects commit, triggers peribolos job

Peribolos applies config

Peribolos prow job



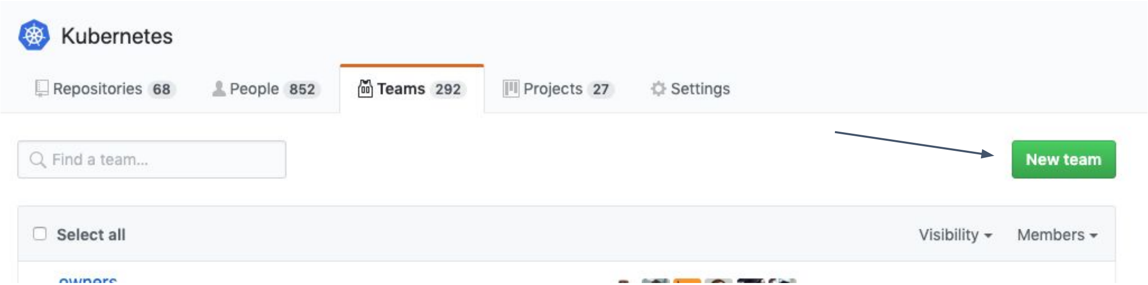
```yaml
postsubmits:
  kubernetes/org:
  - name: post-org-peribolos
    decorate: true
    max_concurrency: 1
    spec:
      containers:
      - image: gcr.io/k8s-prow/peribolos
        args:
        - --config-path=/etc/config/config.yaml
        - --github-token-path=/etc/github-token/oauth
        - --fix-org
        - --confirm
        volumeMounts:
        - name: github
          mountPath: /etc/github-token
          readOnly: true
        - name: config
          mountPath: /etc/config
          readOnly: true
      volumes:
      - name: github
        secret:
          secretName: oauth-token
      - name: config
        configMap:
          name: config
```

Apply declared config

```
peribolos --config-path=org.yaml --github-token-path=$TOKEN --fix-teams # --confirm
```

- Apply current config with gitops
  - Person pushes changes to current config
  - Prow detects change and runs peribolos
  - Peribolos reconciles this new config

Benefits of adoption - Creating a team



Kubernetes

Repositories 68 | People 852 | Teams 292 | Projects 27 | Settings

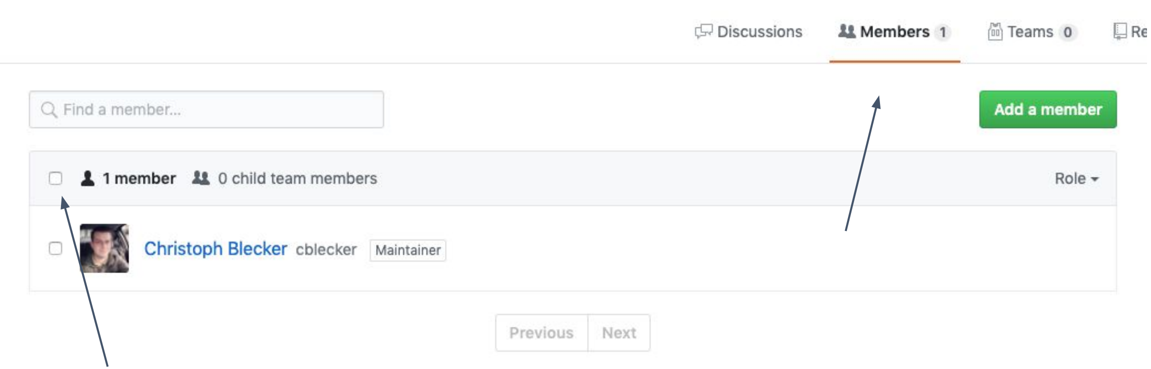
Find a team...

New team

□ Select all

Visibility ▾ Members ▾

owners



Discussions | Members 1 | Teams 0 | Re

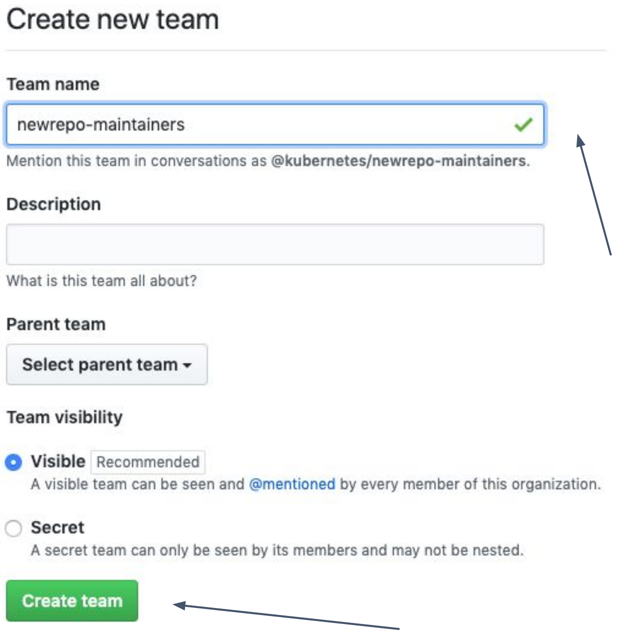
Find a member...

Add a member

□ 1 member 0 child team members Role ▾

□ Christoph Blecker cblecker Maintainer

Previous | Next



Create new team

Team name

newrepo-maintainers ✓

Mention this team in conversations as **@kubernetes/newrepo-maintainers**.

Description

What is this team all about?

Parent team

Select parent team ▾

Team visibility

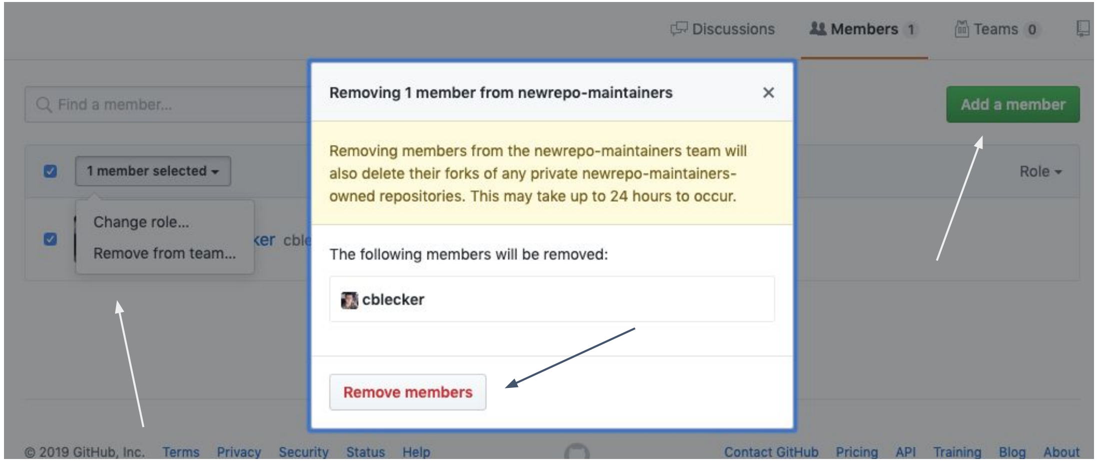
● **Visible** Recommended
A visible team can be seen and @mentioned by every member of this organization.

○ **Secret**
A secret team can only be seen by its members and may not be nested.

Create team

Click Counter: 4

Benefits of adoption - Creating a team

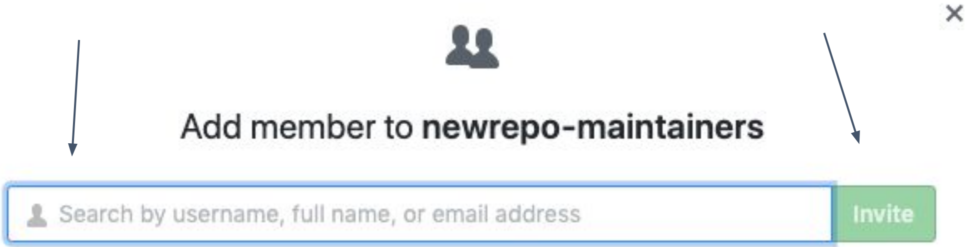


Removing 1 member from newrepo-maintainers

Removing members from the newrepo-maintainers team will also delete their forks of any private newrepo-maintainers-owned repositories. This may take up to 24 hours to occur.

The following members will be removed:

cblecker

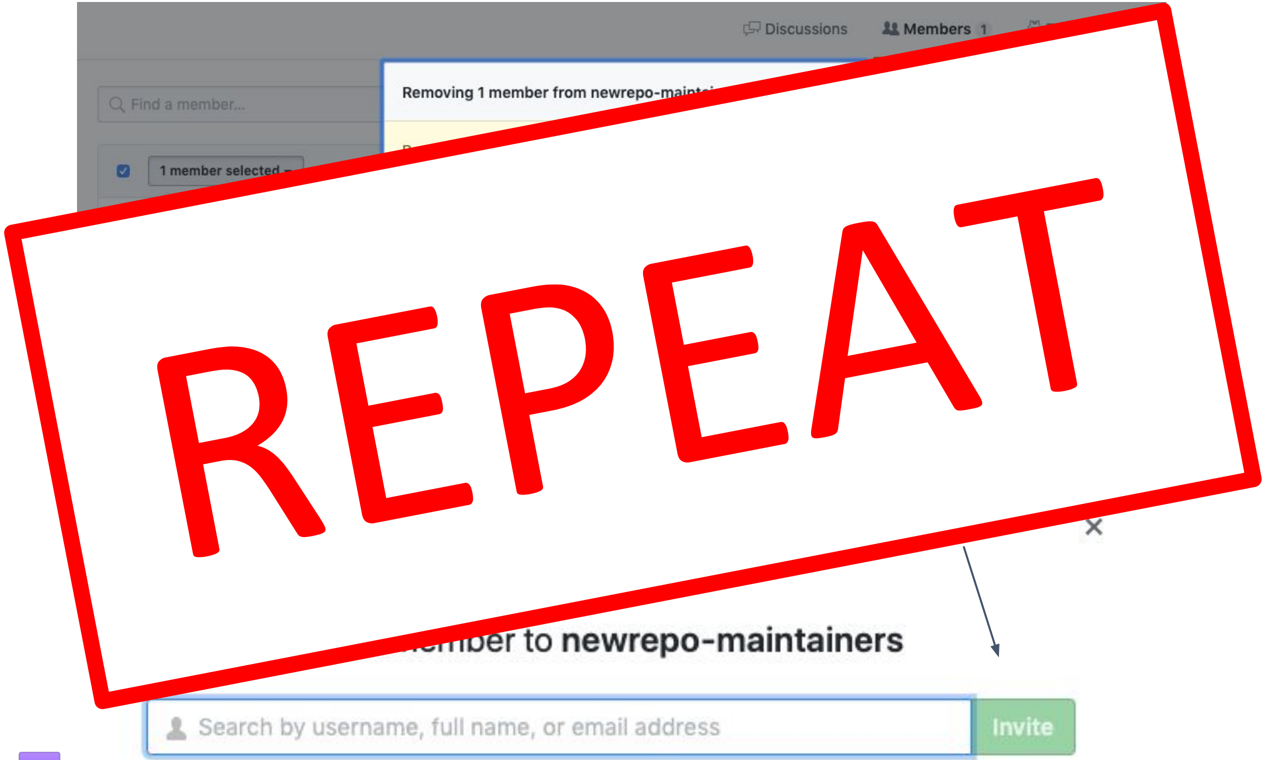


Add member to **newrepo-maintainers**

Click Counter: 80

KubeCon CloudNativeCon Europe 2019

Benefits of adoption - Creating a team



Removing 1 member from newrepo-maint

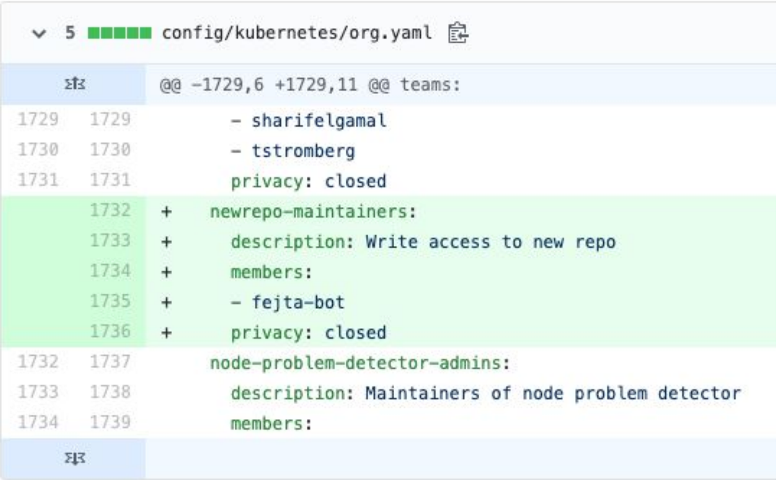
…ember to newrepo-maintainers

Search by username, full name, or email address

REPEAT

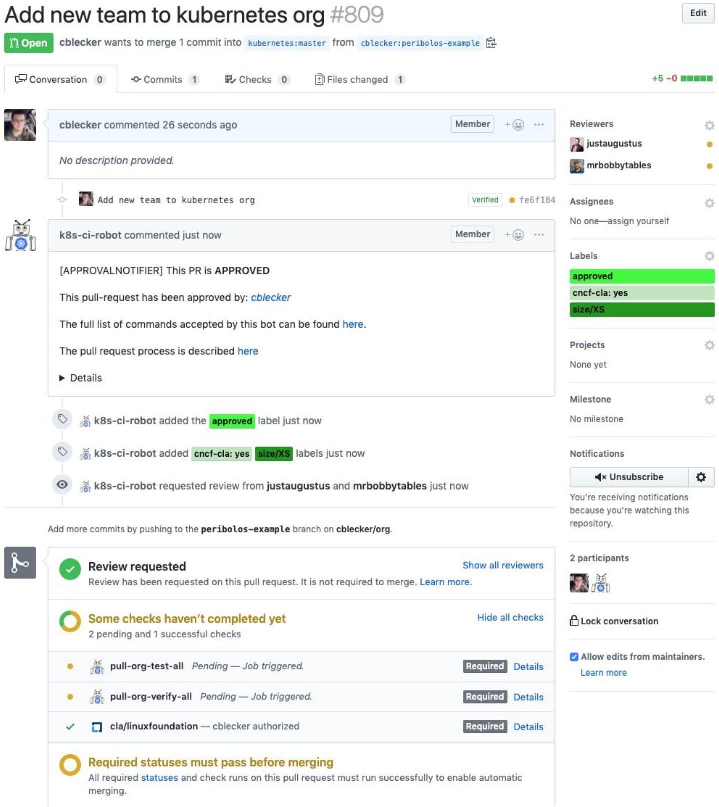
Click Counter: ♾️

Benefits of adoption - Creating a team



5 config/kubernetes/org.yaml

```diff
@@ -1729,6 +1729,11 @@ teams:
          - sharifelgamal
          - tstromberg
        privacy: closed
+     newrepo-maintainers:
+       description: Write access to new repo
+       members:
+         - fejta-bot
+       privacy: closed
      node-problem-detector-admins:
        description: Maintainers of node problem detector
        members:
```



Add new team to kubernetes org #809

Open cblecker wants to merge 1 commit into `kubernetes:master` from `cblecker:peribolos-example`

cblecker commented 26 seconds ago — Member

No description provided.

`Add new team to kubernetes org` Verified ● fe6f184

k8s-ci-robot commented just now — Member

[APPROVALNOTIFIER] This PR is **APPROVED**

This pull-request has been approved by: *cblecker*

The full list of commands accepted by this bot can be found here.

The pull request process is described here

▶ Details

k8s-ci-robot added the approved label just now

k8s-ci-robot added cncf-cla: yes size/XS labels just now

k8s-ci-robot requested review from **justaugustus** and **mrbobbytables** just now

Add more commits by pushing to the **peribolos-example** branch on **cblecker/org**.

✓ **Review requested** — Show all reviewers
Review has been requested on this pull request. It is not required to merge. Learn more.

Some checks haven't completed yet — Hide all checks
2 pending and 1 successful checks

● **pull-org-test-all** *Pending — Job triggered.* Required Details

● **pull-org-verify-all** *Pending — Job triggered.* Required Details

✓ **cla/linuxfoundation** — cblecker authorized Required Details

Required statuses must pass before merging
All required statuses and check runs on this pull request must run successfully to enable automatic merging.

Reviewers
justaugustus ●
mrbobbytables ●

Assignees
No one—assign yourself

Labels
approved
cncf-cla: yes
size/XS

Projects
None yet

Milestone
No milestone

Notifications
Unsubscribe
You're receiving notifications because you're watching this repository.

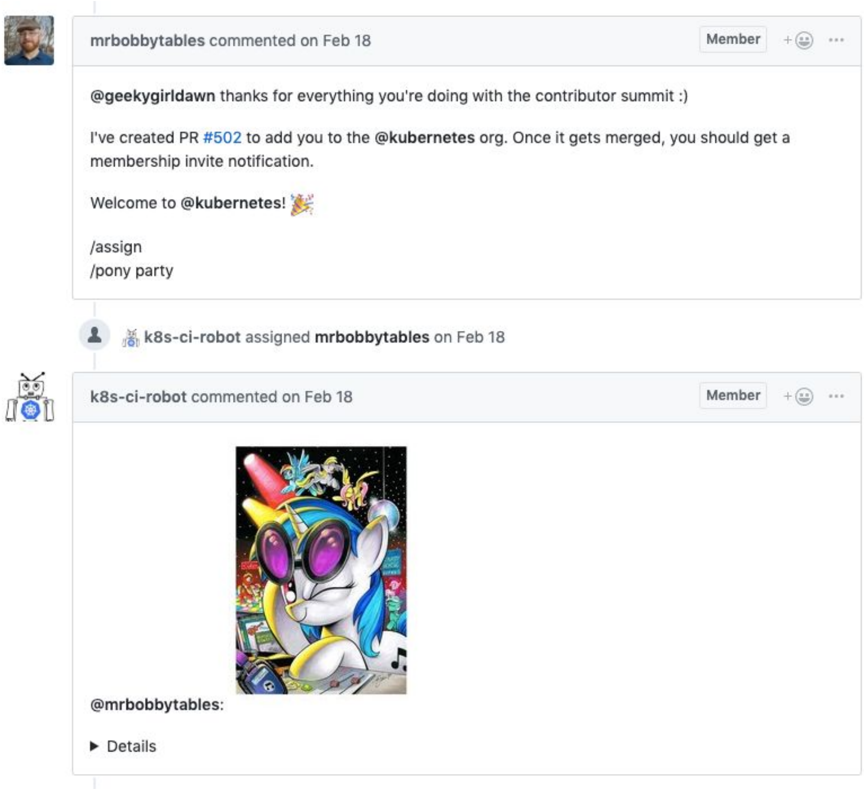
2 participants

Lock conversation

☑ Allow edits from maintainers.
Learn more

Benefits of adoption

- Easier, and faster workflow
- Enforce standards through CI tests
- Clear, public audit trail for all team and membership changes
- Code review workflow allows for delegation of privileges; faster time to process
- More Pony GIFs



mrbobbytables commented on Feb 18 · Member

@geekygirldawn thanks for everything you're doing with the contributor summit :)

I've created PR #502 to add you to the **@kubernetes** org. Once it gets merged, you should get a membership invite notification.

Welcome to **@kubernetes**! 🎉

/assign
/pony party

k8s-ci-robot assigned **mrbobbytables** on Feb 18

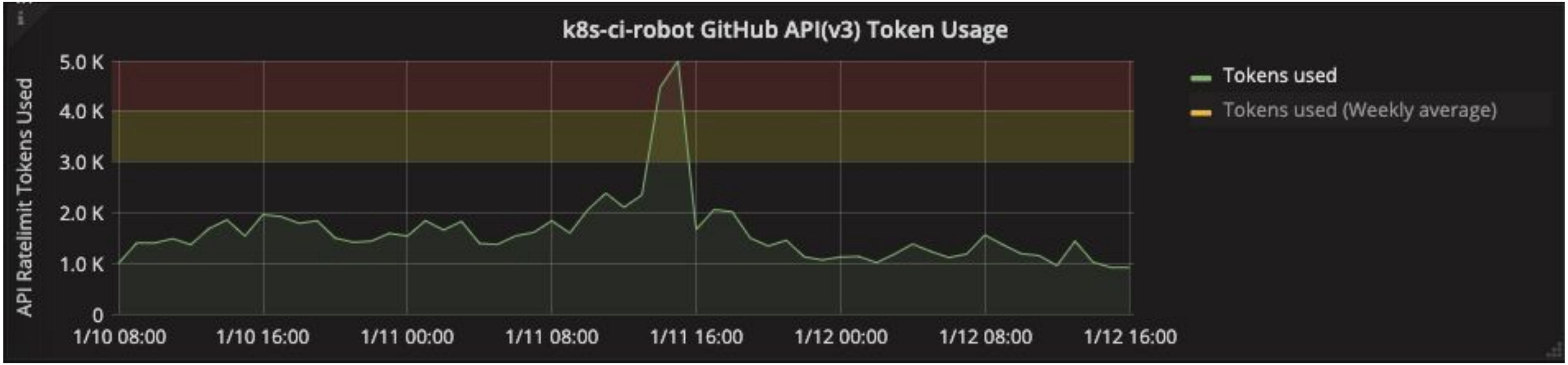
k8s-ci-robot commented on Feb 18 · Member

@mrbobbytables:

▸ Details

Issues we've encountered

- Token Usage



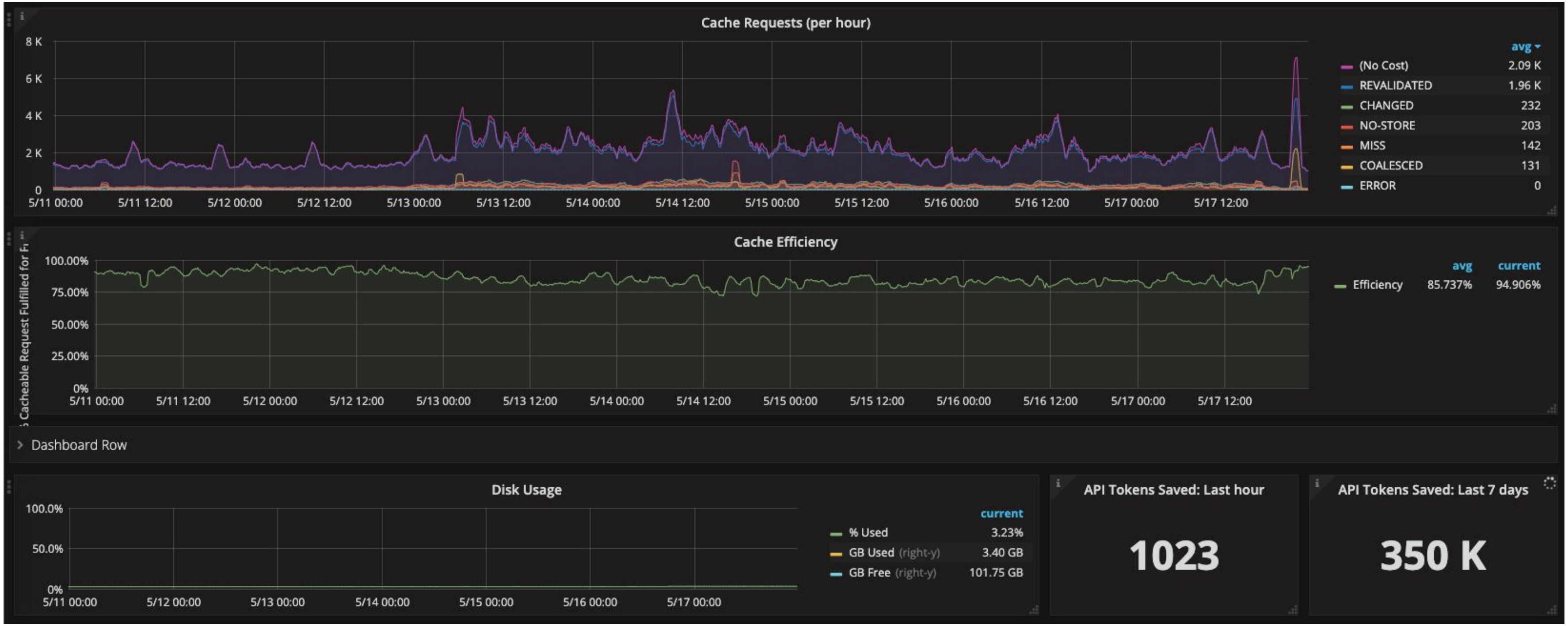
Issues we’ve encountered

- Token Usage

```
$ docker run gcr.io/k8s-prow/peribolos --help 2>&1 | grep -A3 -e ' -token-burst'
  -token-burst int
        Allow consuming a subset of hourly tokens in a short burst (default 100)
  -tokens int
        Throttle hourly token consumption (0 to disable) (default 300)
```

Issues we’ve encountered

- Token Usage



Cache Requests (per hour)

	avg
(No Cost)	2.09 K
REVALIDATED	1.96 K
CHANGED	232
NO-STORE	203
MISS	142
COALESCED	131
ERROR	0

Cache Efficiency

	avg	current
Efficiency	85.737%	94.906%

Dashboard Row

Disk Usage

	current
% Used	3.23%
GB Used (right-y)	3.40 GB
GB Free (right-y)	101.75 GB

API Tokens Saved: Last hour

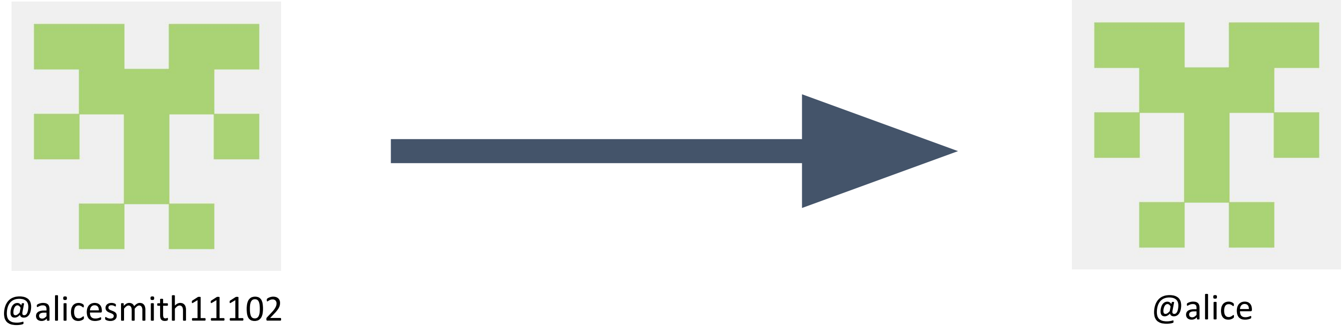
1023

API Tokens Saved: Last 7 days

350 K

Issues we’ve encountered

- Username changes

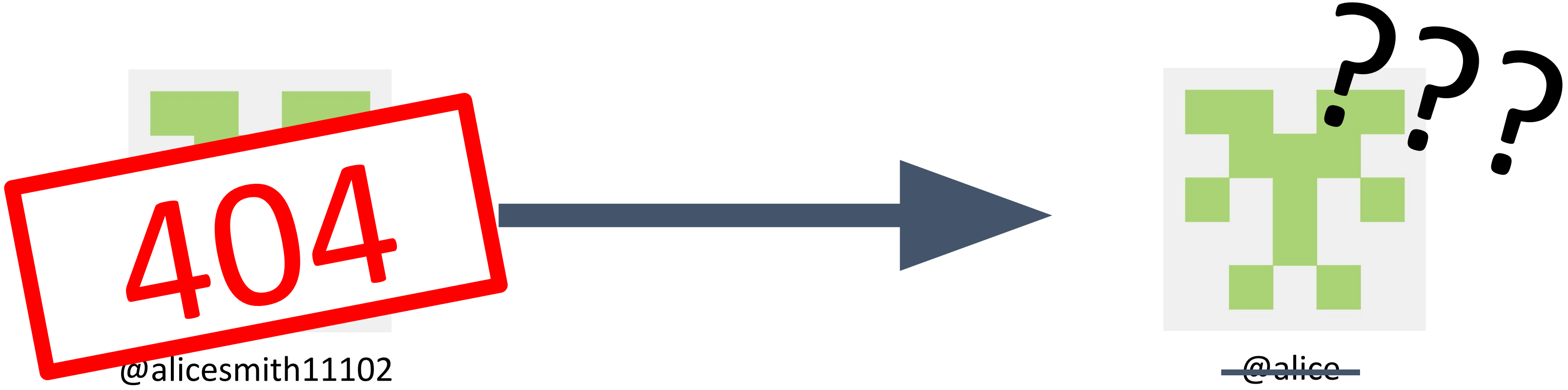


@alicesmith11102

@alice

Issues we’ve encountered

- Username changes



@alicesmith11102

~~@alice~~

Where do we go from here

Manage repos

Better concurrency mitigations

Better delegation

How do I get started?

Source code: https://git.k8s.io/test-infra/prow/cmd/peribolos

Our public GitHub configuration: https://git.k8s.io/org

Slides from this talk: https://sched.co/MPZA

Contact information:

#sig-contribex, #sig-testing, #prow on slack.k8s.io

@cblecker and @fejta on Slack/GitHub