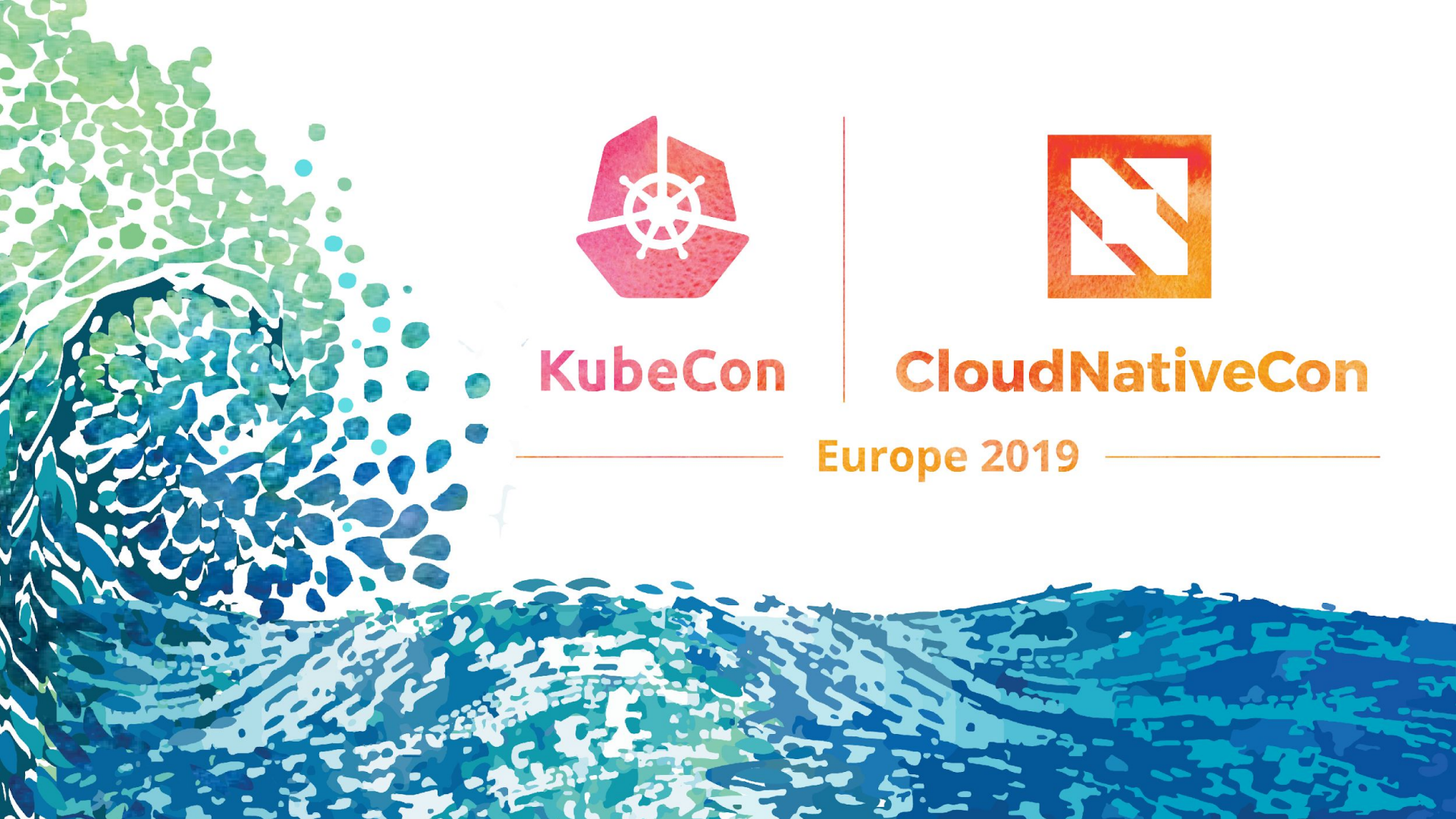
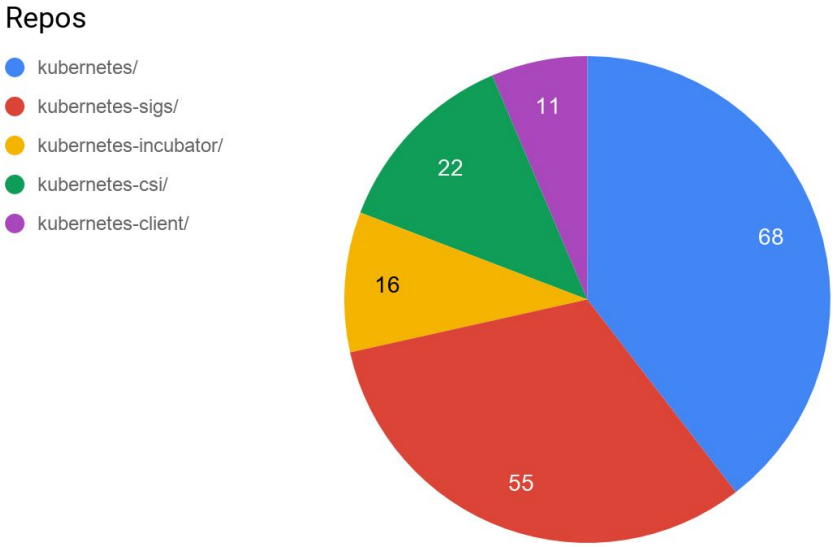

KubeCon
CloudNativeCon
Europe 2019

Peribolos

How Kubernetes uses gitops to manage GitHub communities at scale

Christoph Blecker, Red Hat
Erick Fejta, Google

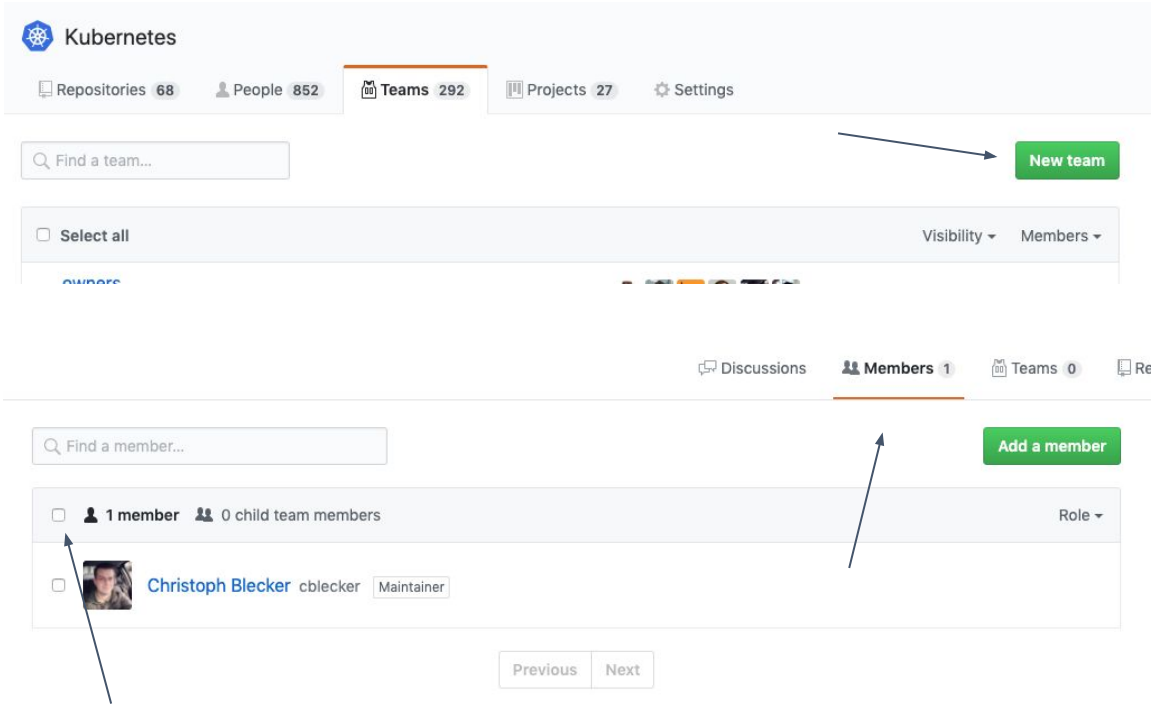
Kubernetes GitHub footprint

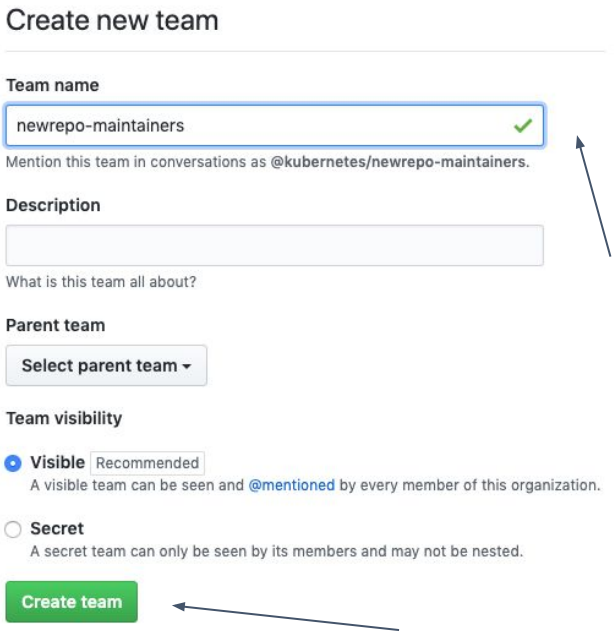


As of May 2019:

- 5 primary orgs
- ~ 175 repos
- 500+ GitHub teams
- 930+ unique members
- Over 170 new members in the first five months of this year

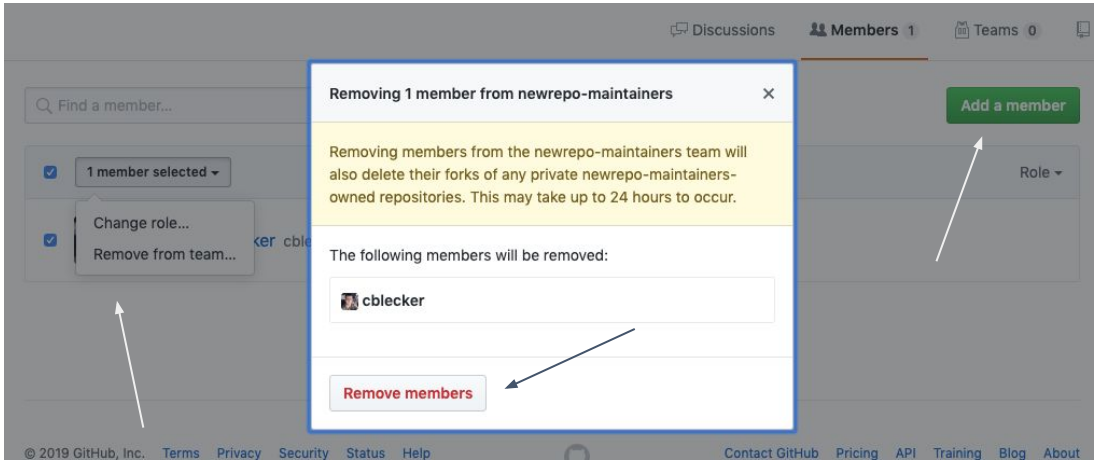
Creating a team - Checkboxes everywhere

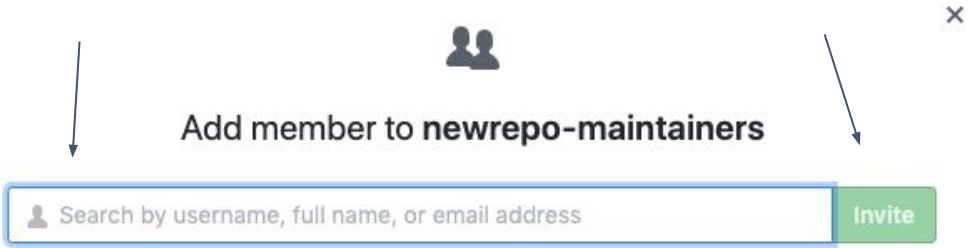




Click Counter: 8

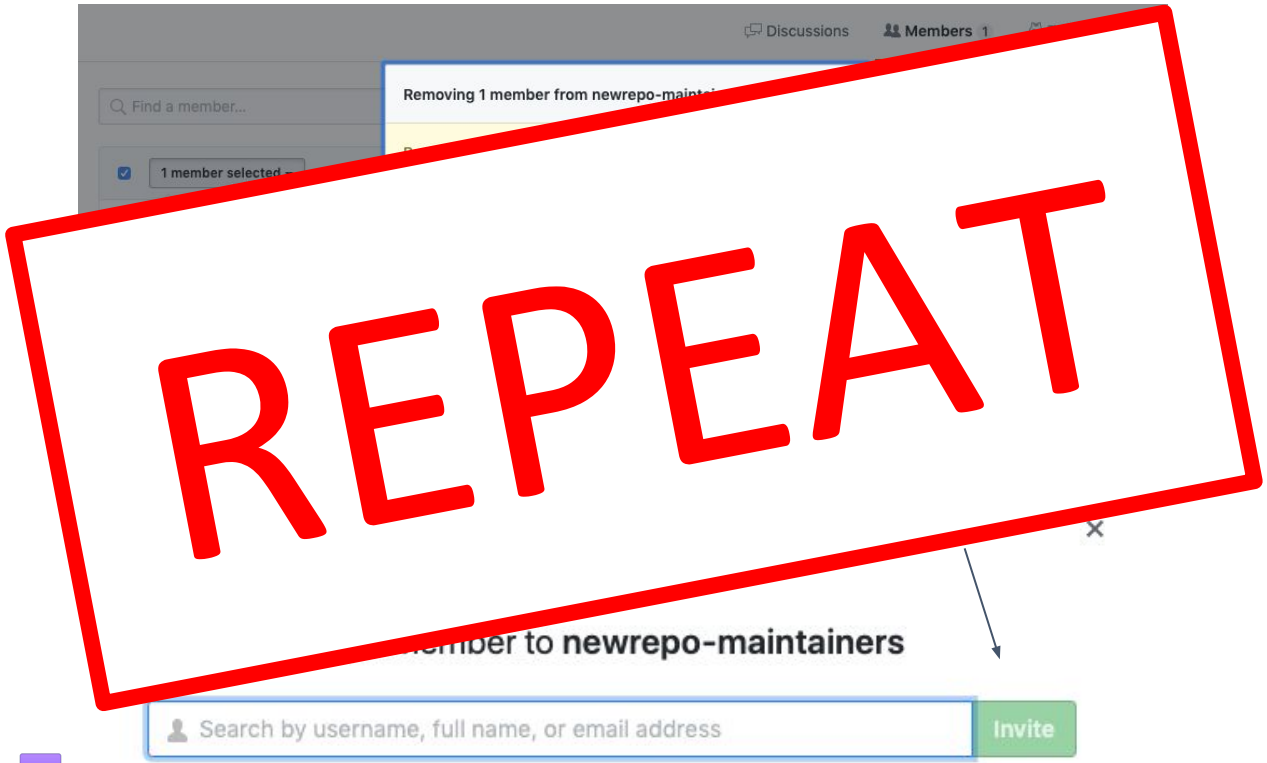
Creating a team - Checkboxes everywhere





Click Counter: 10

Checkboxes everywhere - Creating a team



Click Counter: ∞

Challenges:

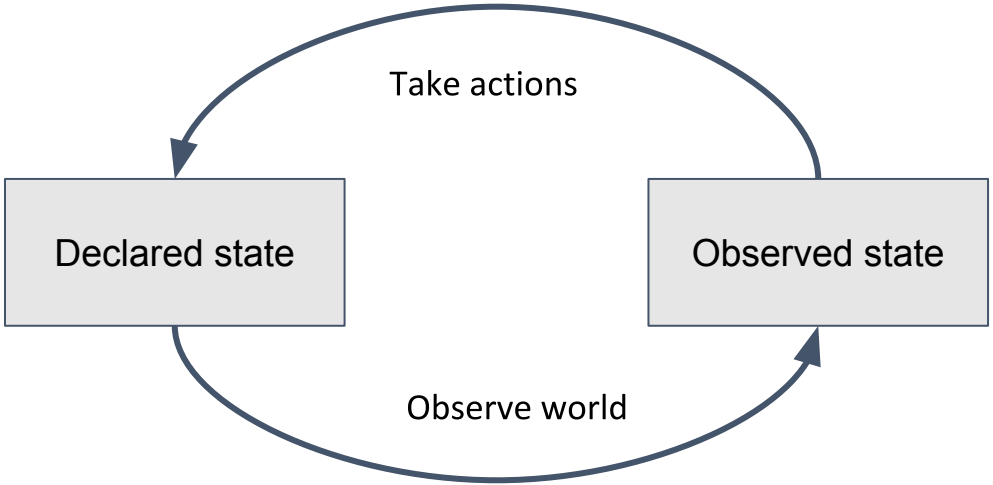
- Limited access levels -- many changes require “owner” privileges
- Settings spread across many different web pages
- Multi-screen processes to accomplish goals
- No visibility to changes outside of sensitive audit logs

Goals:

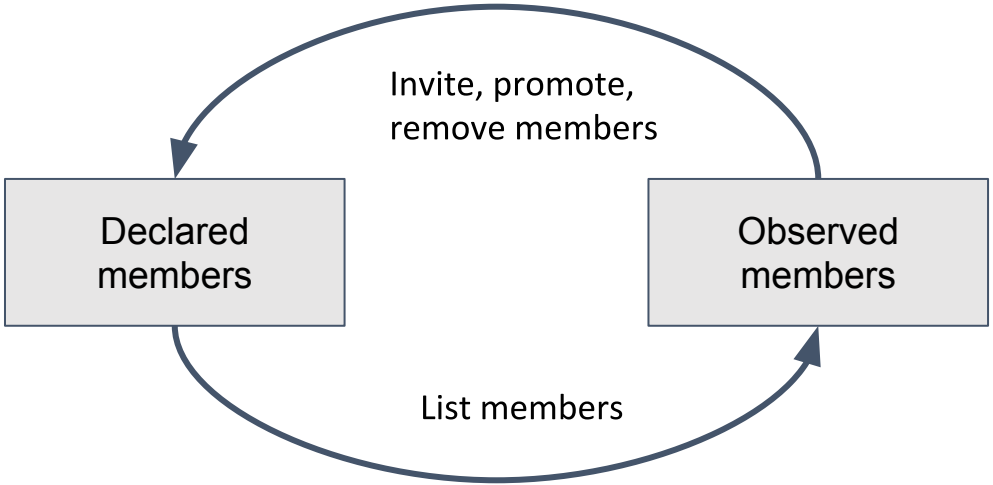
- Clear and simple exposure of settings
- Ability to make changes settings across all orgs
- Visibility and audit trail into changes
- Periodic reconciliation of desired state
- Delegation of privilege wherever possible
- Accomplish this in a *safe* way

I’m sorry Dave, I’m afraid I can’t do that.

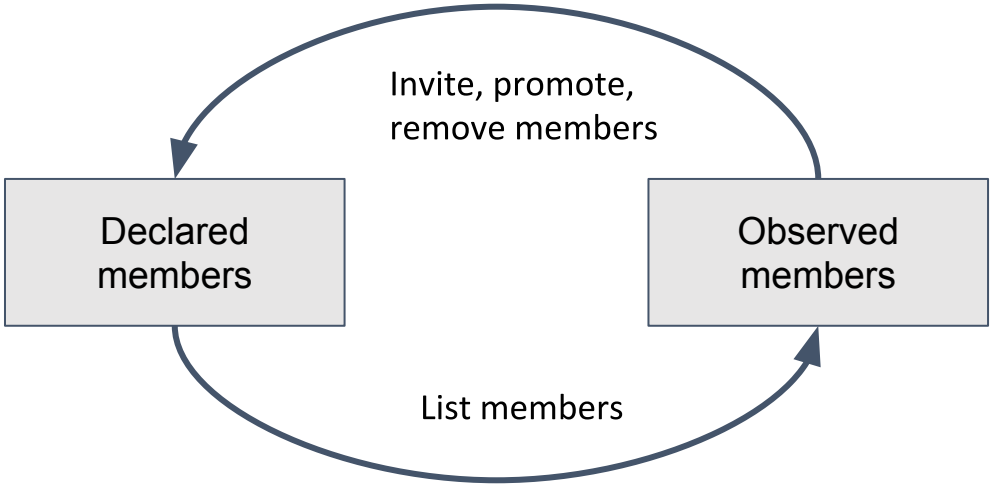
kubernetes reconciliation loop



org reconciliation loop



org reconciliation loop



Repeat for metadata, teams, etc

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

```
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
- Manage org metadata, teams, members
  - Convenient to edit
- while true; do
  - Update file to desired state
  - Reconcile desired and actual state
- Safe to run

Getting started

docker run gcr.io/k8s-prow/peribolos --help

go get -u k8s.io/test-infra/prow/cmd/peribolos

git clone https://github.com/test-infra.git && bazel build //prow/cmd/peribolos

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

```
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
```

```
{"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"}
```

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)

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

- Apply current config
  - Read desired state
  - Get current state in github
  - Make any changes

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

Designed for Convenience

- Re-entrant
  - Fix code or config and try again
- Config optimized for humans
  - Unique team names (not IDs)
  - Skip managing uninteresting/secret metadata
- Delegate to SIGs
  - Self-service inside their own folder via OWNERS

docker run gcr.io/k8s-prow/peribolos --help

go get -u k8s.io/test-infra/prow/cmd/peribolos

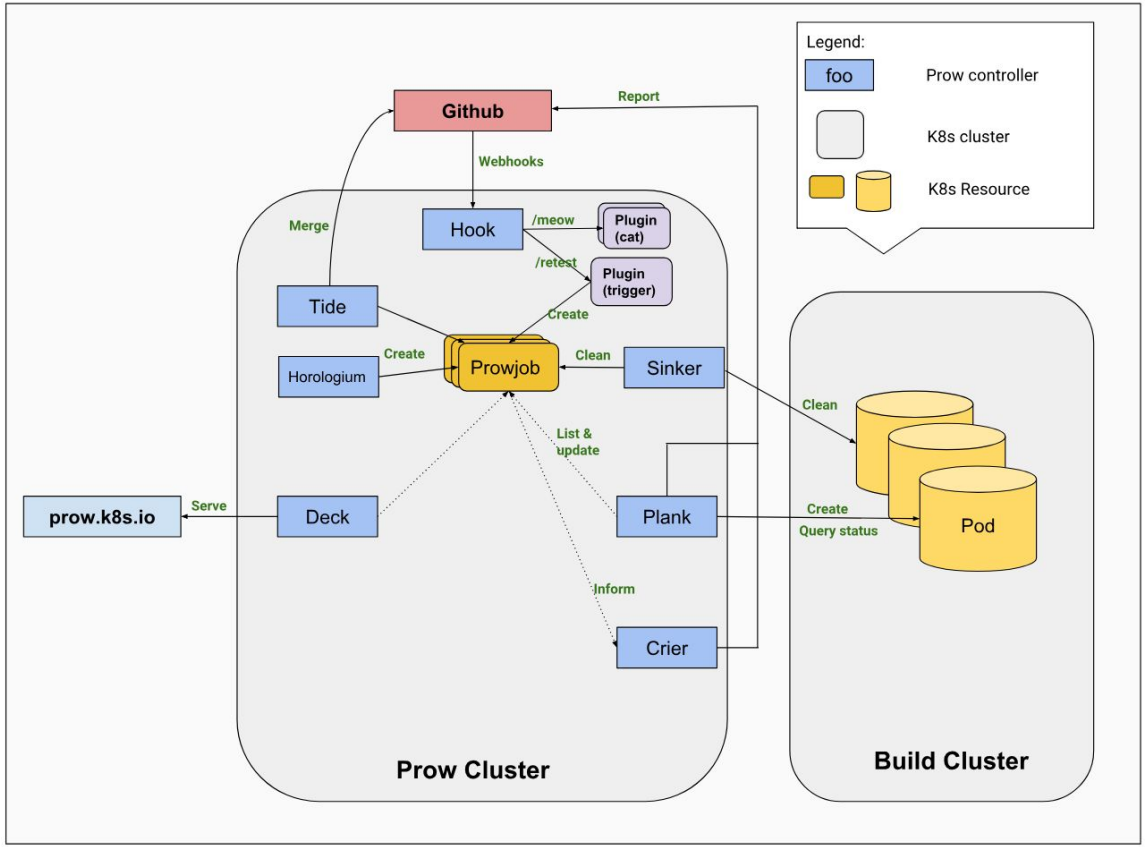
bazel build //prow/cmd/peribolos

Safety mitigations

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

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

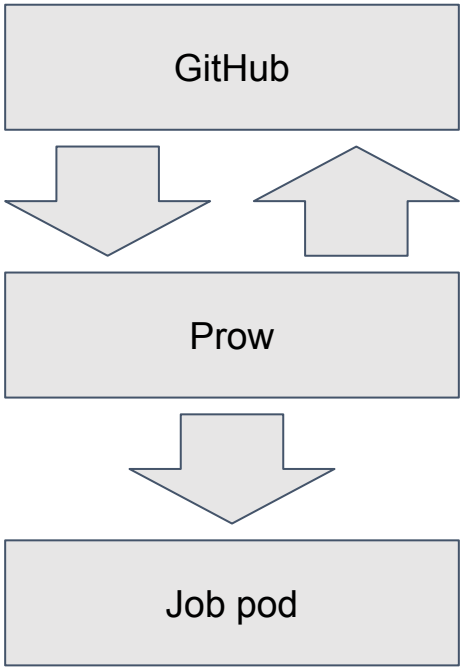
- ~~Apply current config~~
- Apply current config **with gitops**


Legend:
foo
Prow controller
K8s cluster
K8s Resource
Github
Report
Webhooks
Merge
Hook
/meow
Plugin (cat)
/retest
Plugin (trigger)
Tide
Create
Create
Horologium
Prowjob
Clean
Sinker
Clean
List & update
prow.k8s.io
Serve
Deck
Plank
Create
Query status
Pod
Inform
Crier
Prow Cluster
Build Cluster

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

Github Events:

- Merge PR
- Push commit
- Left comment



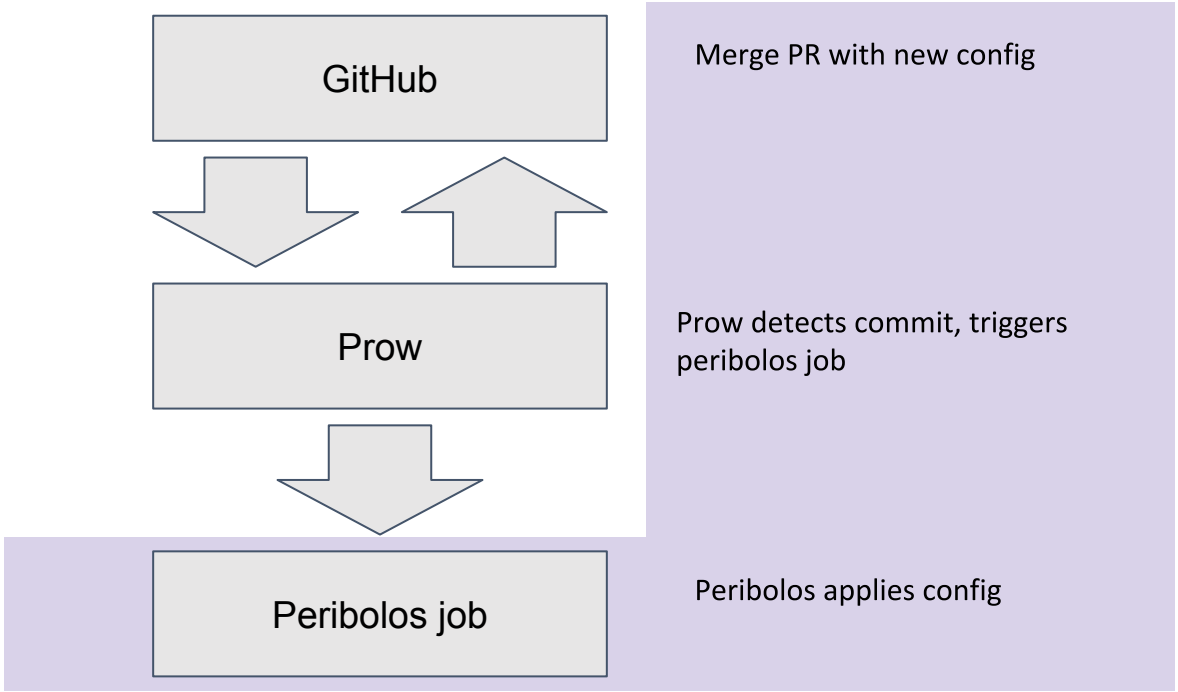
Prow Responses:

- Update status context
- Leave comment
- Change labels

Prow actions

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

Prow + peribolos



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
```

https://github.com/kubernetes/test-infra/tree/master/config/jobs/kubernetes/org

Creating a team - Let's try that again

5 config/kubernetes/org.yaml

```
@@ -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

Edit

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

Conversation 0 · Commits 1 · Checks 0 · Files changed 1 · +5 −0

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

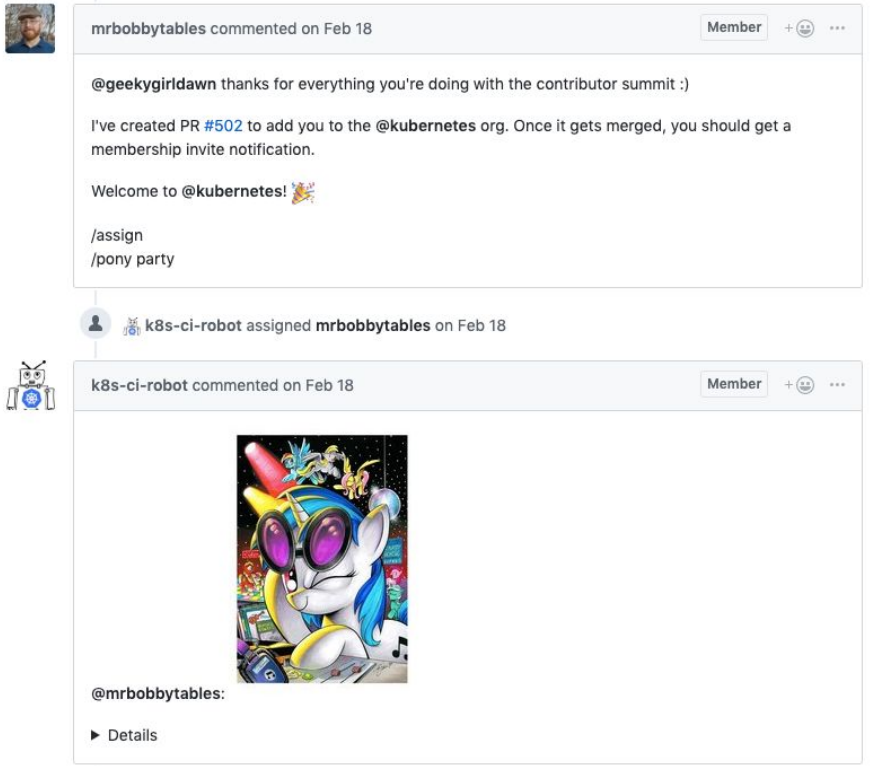
You're receiving notifications because you're watching this repository.

2 participants

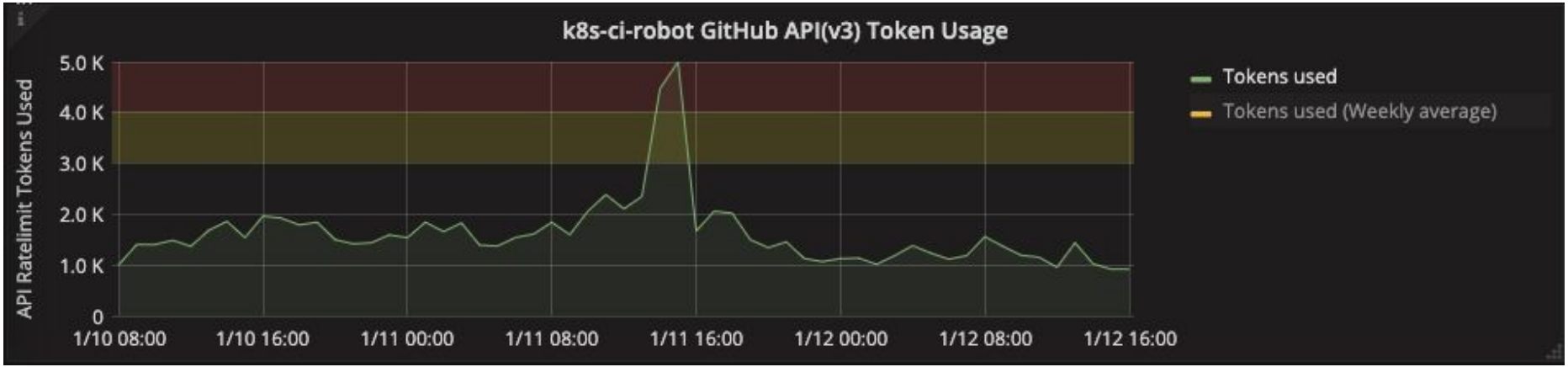
Lock conversation

Allow edits from maintainers. Learn more

- 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



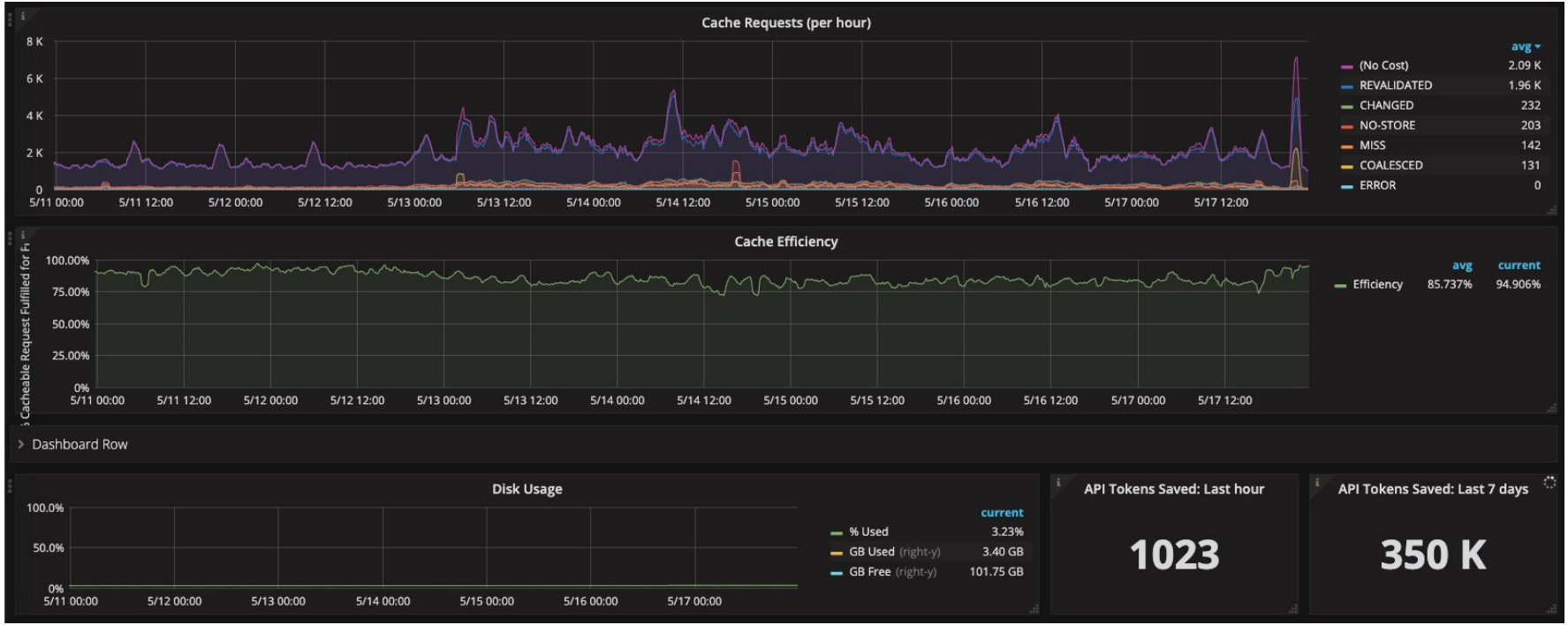
- Token Usage


k8s-ci-robot GitHub API(v3) Token Usage
API Ratelimit Tokens Used
5.0 K
4.0 K
3.0 K
2.0 K
1.0 K
0
1/10 08:00
1/10 16:00
1/11 00:00
1/11 08:00
1/11 16:00
1/12 00:00
1/12 08:00
1/12 16:00
Tokens used
Tokens used (Weekly average)

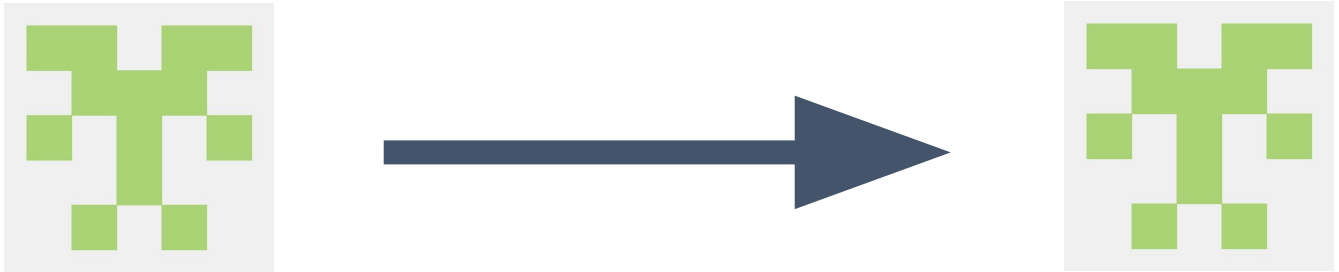
- Token Usage

```
$ 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)
```

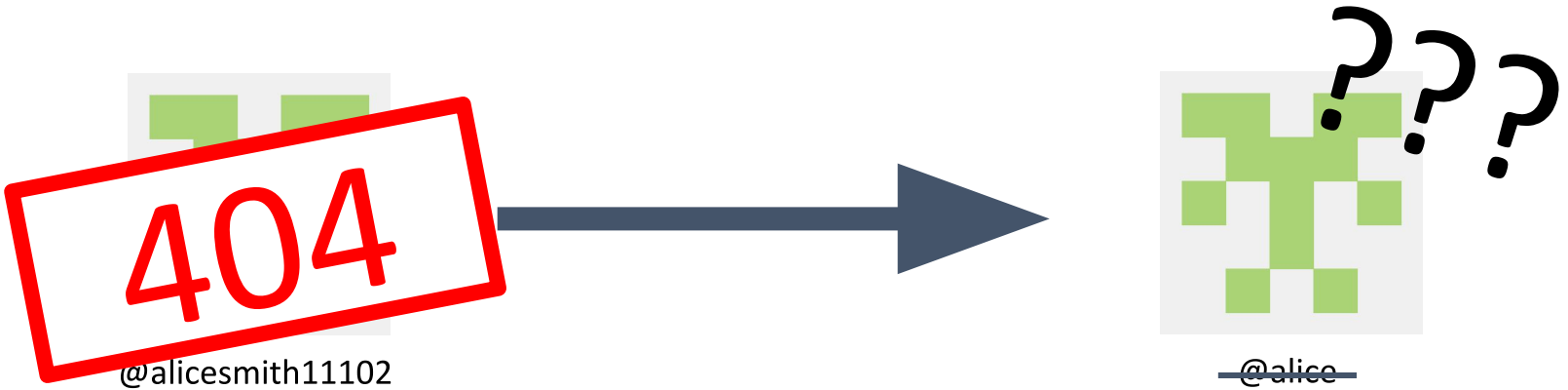
- Token Usage


Cache Requests (per hour)
8 K
6 K
4 K
2 K
0
5/11 00:00
5/11 12:00
5/12 00:00
5/12 12:00
5/13 00:00
5/13 12:00
5/14 00:00
5/14 12:00
5/15 00:00
5/15 12:00
5/16 00:00
5/16 12:00
5/17 00:00
5/17 12:00
avg
(No Cost) 2.09 K
REVALIDATED 1.96 K
CHANGED 232
NO-STORE 203
MISS 142
COALESCED 131
ERROR 0
Cache Efficiency
Cacheable Request Fulfilled for F
100.00%
75.00%
50.00%
25.00%
0%
avg current
Efficiency 85.737% 94.906%
Dashboard Row
Disk Usage
100.0%
50.0%
0%
5/11 00:00
5/12 00:00
5/13 00:00
5/14 00:00
5/15 00:00
5/16 00:00
5/17 00:00
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

- Username changes



- Username changes



Manage repos

Better concurrency mitigations

Better delegation

Try it: `docker run gcr.io/k8s-prow/peribolos --help`

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

The Kubernetes 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

Questions?