

GitOps Safety: Rendering Accurate Argo CD Diffs Directly on Pull Requests



Regina Voloshin

OSS Tech Lead @ Codefresh by Octopus Deploy

Argo CD Maintainer

CNCF Ambassador

Codefresh GitOps by Octopus Deploy



- Argo Control plane and Promotions

Model app promotions

- Argo Enterprise Support & TAM

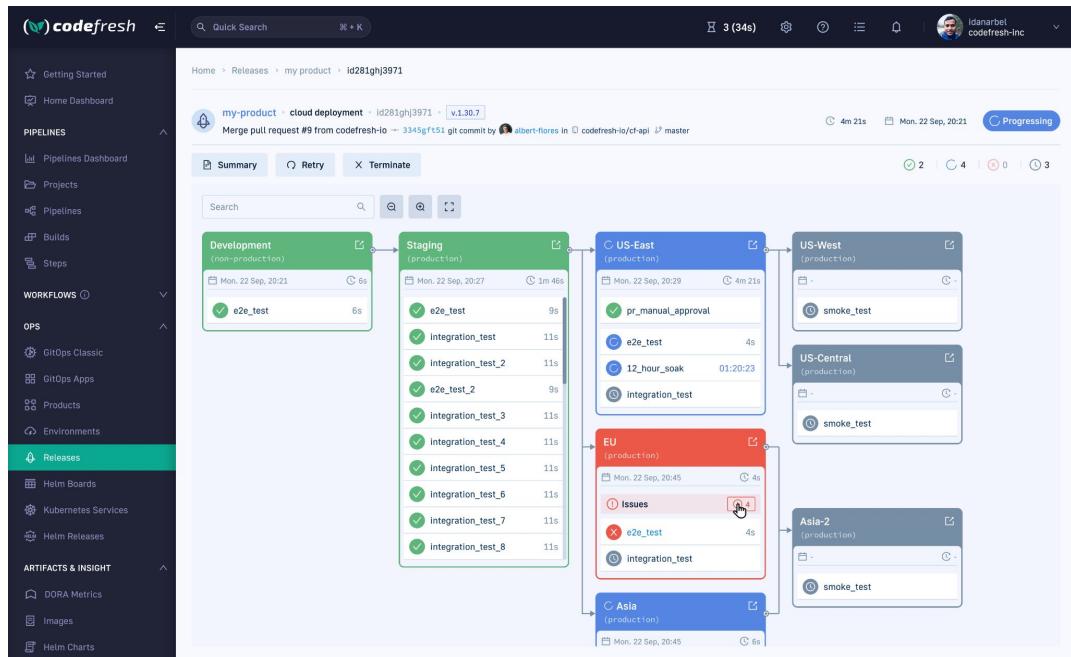
Expert help from Argo Maintainers

- Hardened Security Distro for Argo

Aggressive patching SLA form #1 security maintainers

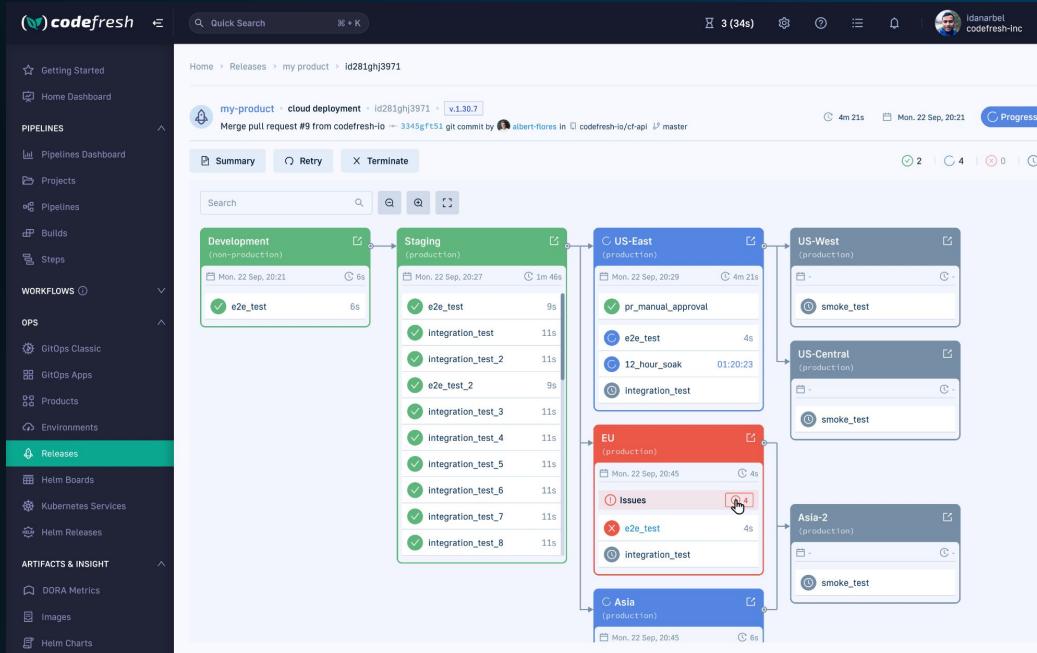
- #1 GitOps Training & Certification

Over 23k students...



Codefresh GitOps by Octopus Deploy

- Argo Control plane and Promotions
Model app promotions
- Argo Enterprise Support & TAM
Expert help from Argo Maintainers
- Hardened Security Distro for Argo
Aggressive patching SLA form #1 security maintainers
- #1 GitOps Training & Certification
Over 23k students...



Fun stats



- Other girls in my high school class:
 - 0
- Hours on a plane on my way here:
 - 18
- Times in KubeCon so far:
 - 0
- Number of things I can do in parallel:
 - 1

Problem: Kustomize Base Change



Open reggie-k wants to merge 1 commit into `main` from `reggie-k-patch-6` ⚙

Conversation 0 Commits 1 Checks 0 Files changed 1

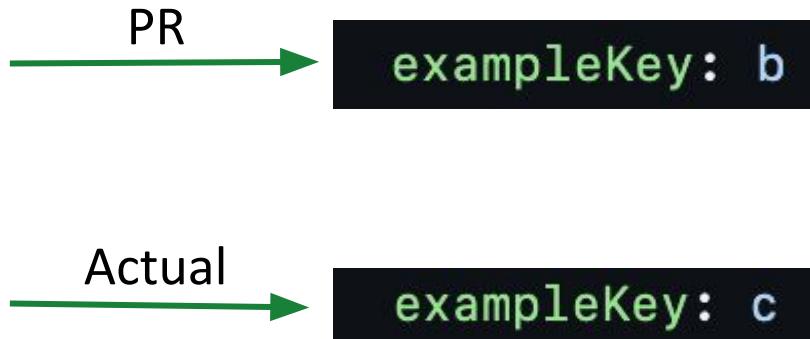
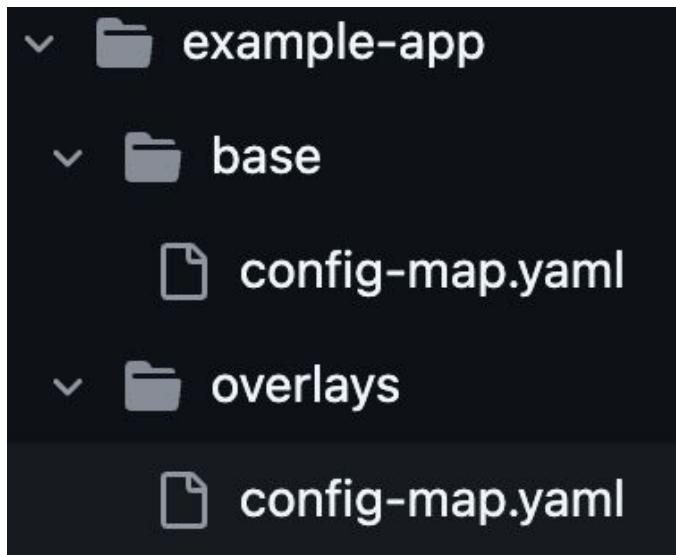
Changes from all commits ▾ File filter ▾ Conversations ▾ Jump to ▾ ⚙ Review ▾

ArgoCon-NA-2024/example-app/base/config-map.yaml

Viewed ⚙ ...

```
@@ -3,5 +3,5 @@ kind: ConfigMap
 3   metadata:
 4     name: example
 5   data:
 6   -   exampleKey: a
 7
 3   metadata:
 4     name: example
 5   data:
 6   +   exampleKey: b
 7
```

Problem: Kustomize Base Change



Problem: Helm Chart Version Change



!! Open reggie-k wants to merge 1 commit into `main` from `reggie-k-patch-7` ⚙

Conversation 0 Commits 1 Checks 0 Files changed 1 +1 -1

Changes from all commits ▾ File filter ▾ Conversations ▾ Jump to ▾ ⚙ 0 / 1 files viewed Review in codespace Review changes ▾

ArgoCon-NA-2024/nginx/nginx-app.yaml ⚙ Viewed ...

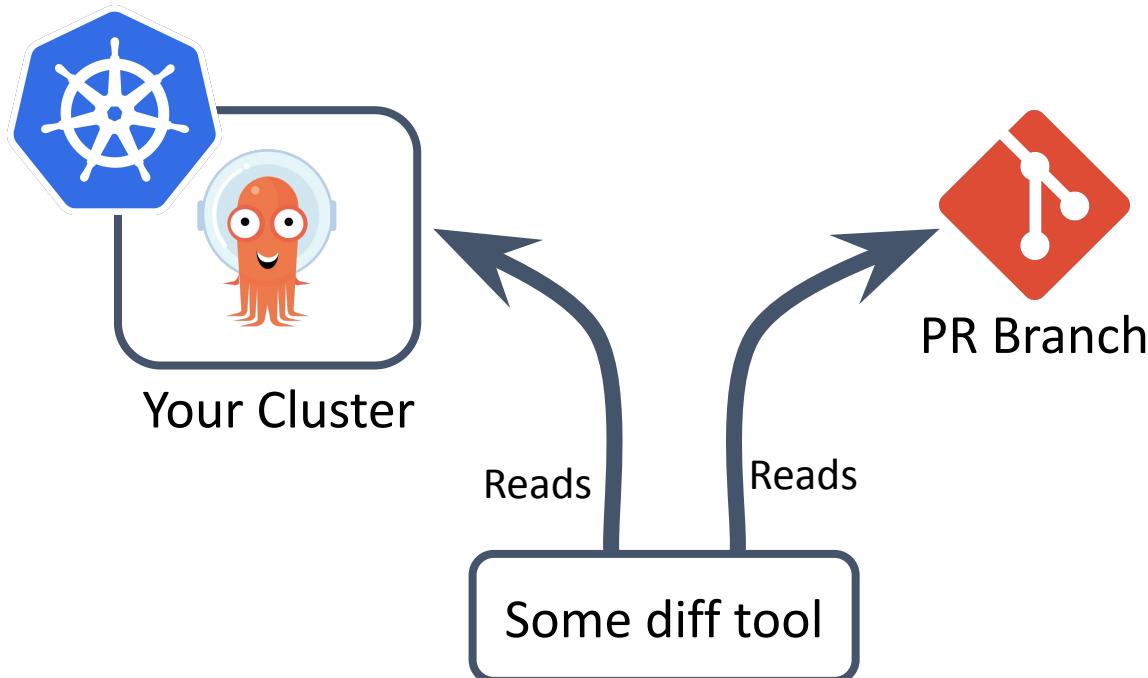
```
@@ -11,7 +11,7 @@ spec:  
11     source:  
12       chart: ingress-nginx  
13       repoURL: https://kubernetes.github.io/ingress-nginx  
14     - targetRevision: 3.41.0  
15     syncPolicy:  
16       automated: {}  
17     syncOptions:  
11     source:  
12       chart: ingress-nginx  
13       repoURL: https://kubernetes.github.io/ingress-nginx  
14     + targetRevision: 4.11.3  
15     syncPolicy:  
16       automated: {}  
17     syncOptions:
```

Full visibility on the diff!

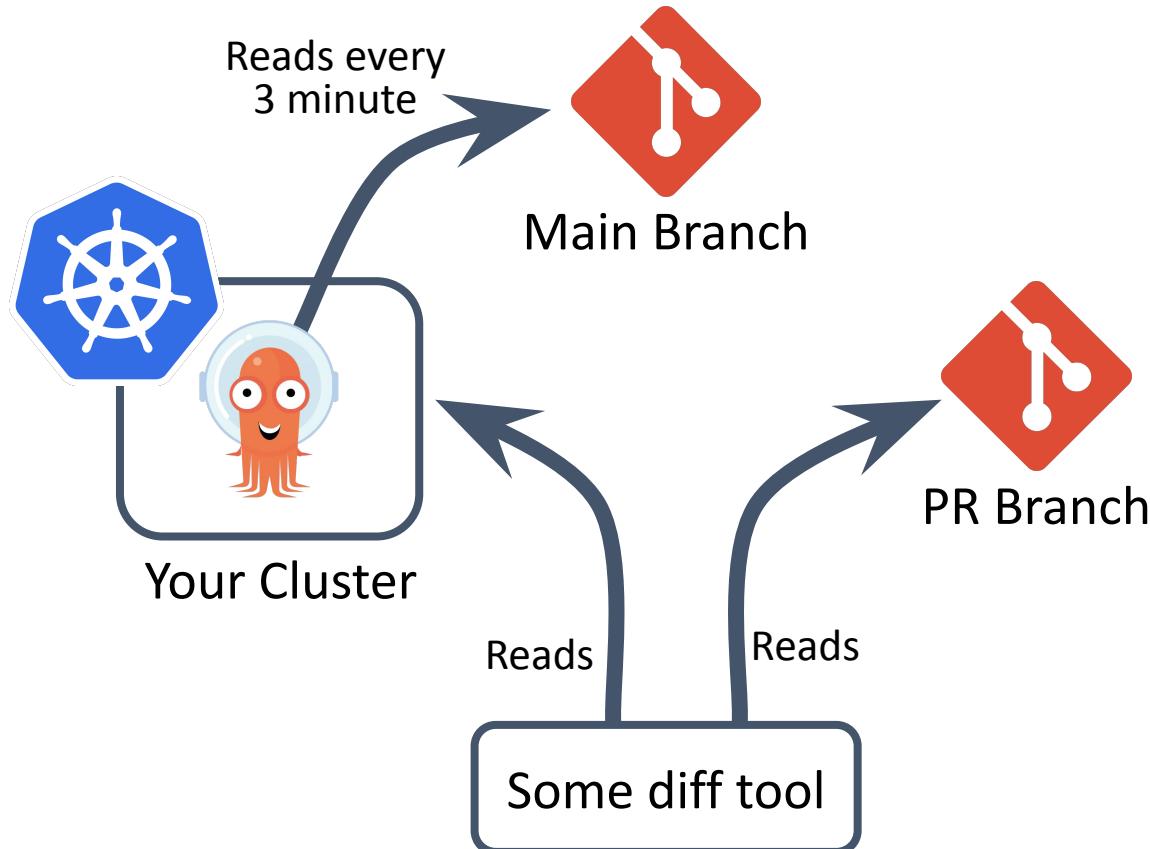
Desired state vs live state

When rendering diffs

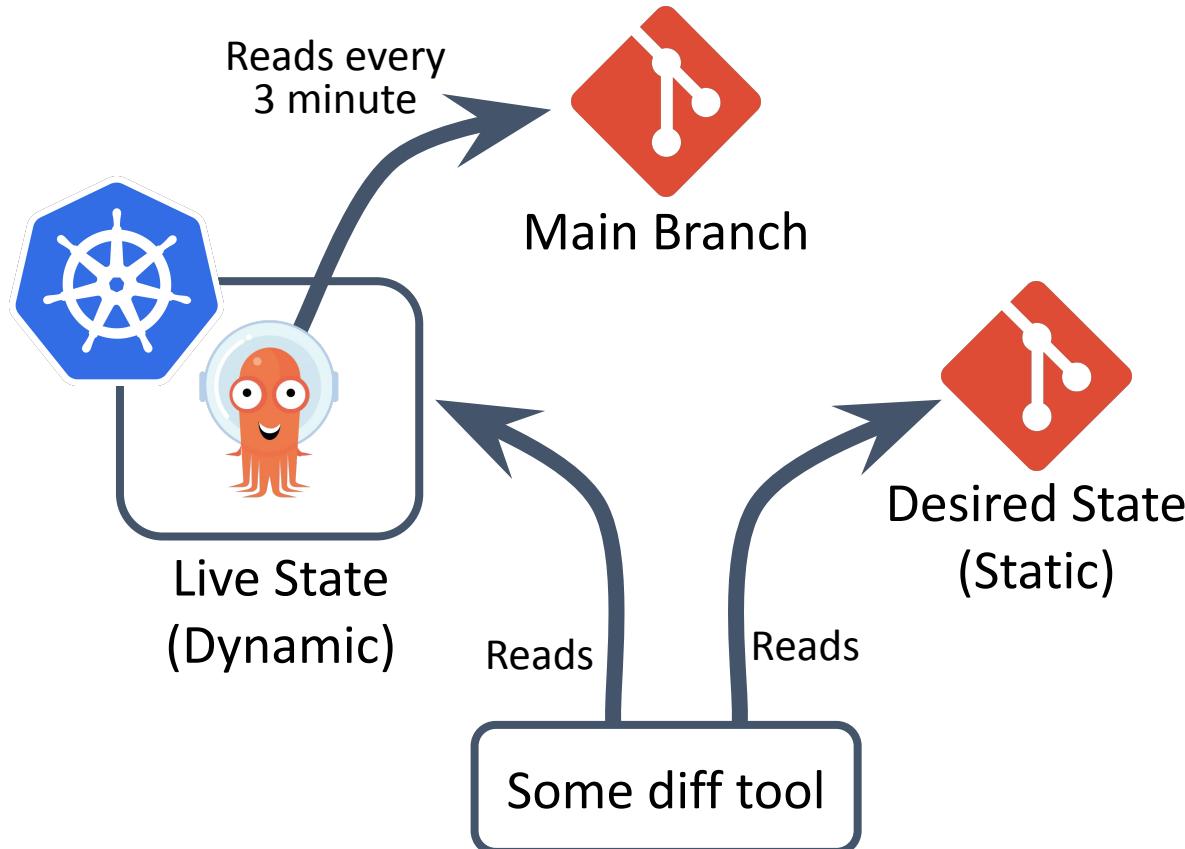
Desired state vs live state



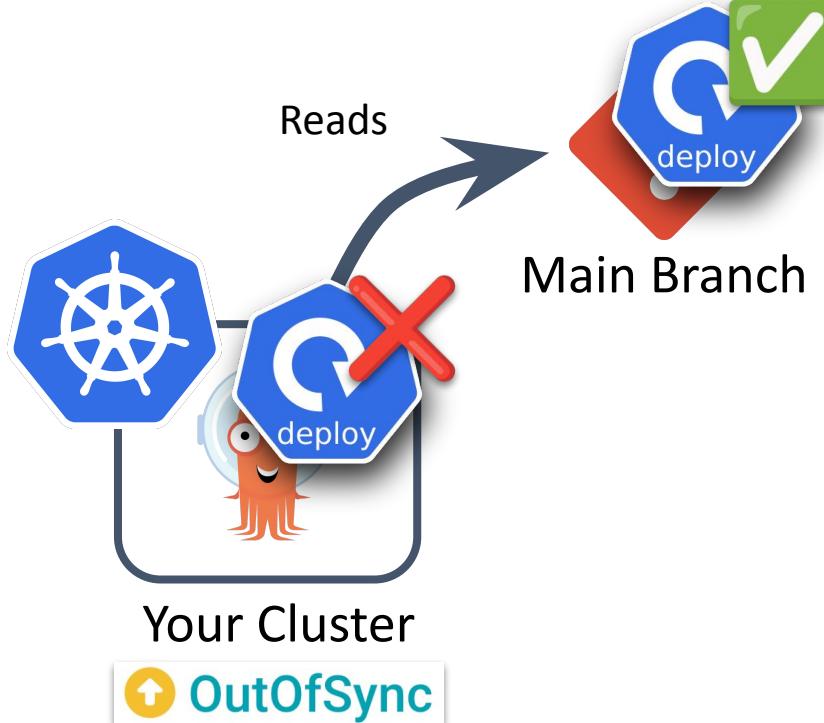
Desired state vs live state



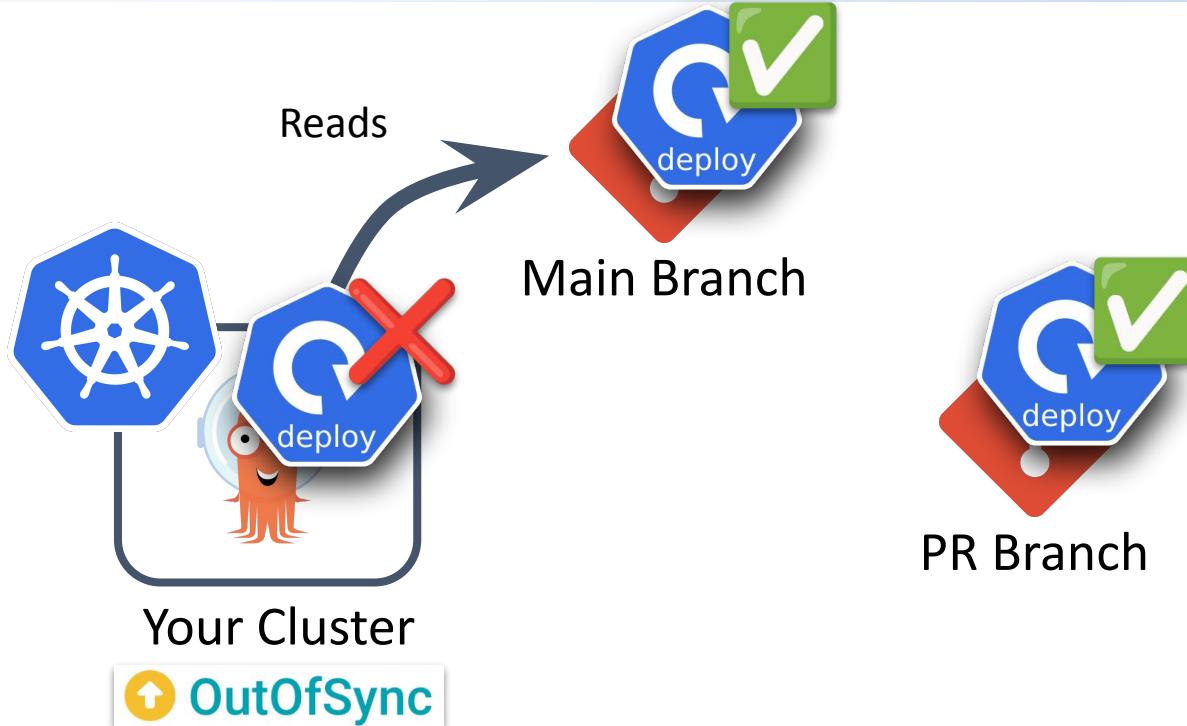
Desired state vs live state



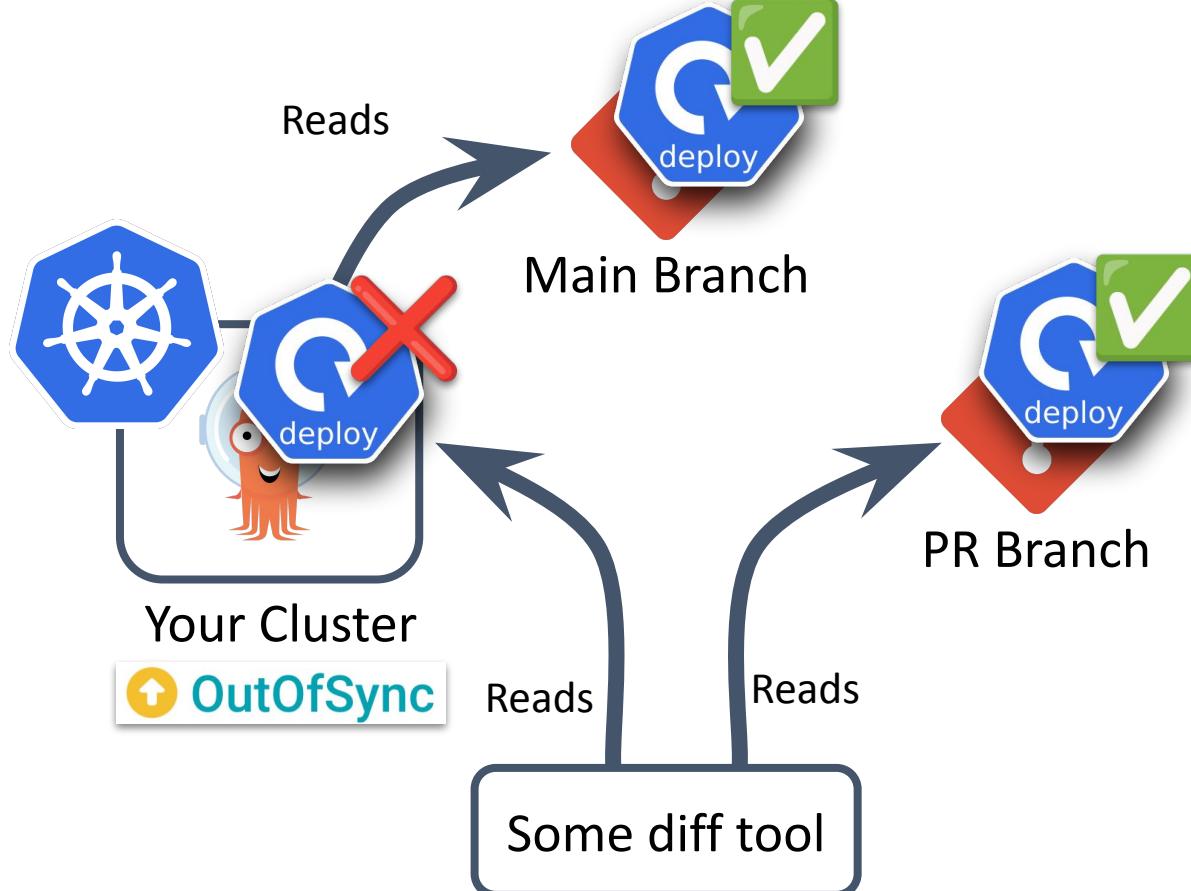
Example



Example

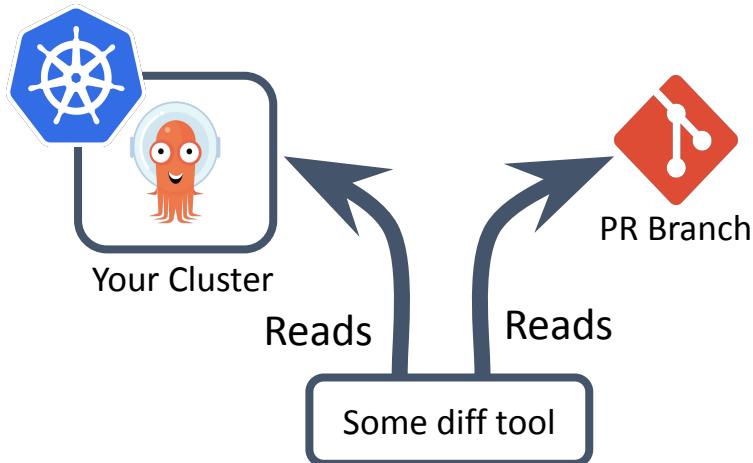


Example

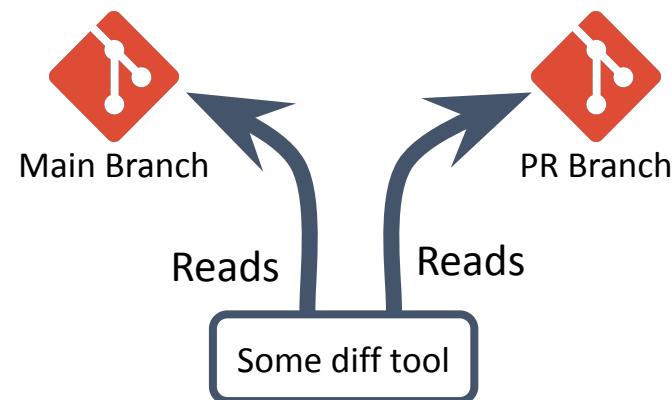


Desired state vs live state

Less predictable



Deterministic



Existing Approaches

For previewing manifests

Approach: Rendered Manifests



Works with



Helm and Kustomize



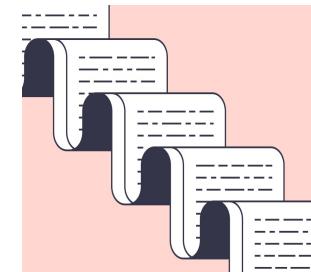
Looks at



fully rendered plain manifests

Enables comparing: desired state to desired state

[Link](#)



Tool: Kubechecks



- K8s Deployment
- Clones the repository
- Runs checks
- Comments results on the PR
- Compares: desired state to live state

[Link](#)

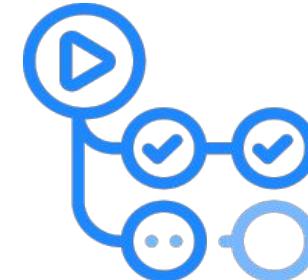
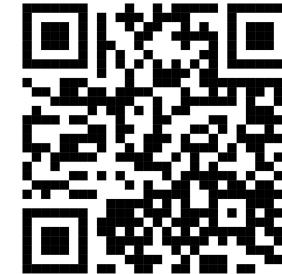


Tool: ArgoCD Diff Action



- GitHub action
- Runs the `argocd diff` command
- Compares: desired state to live state
- Isn't actively maintained lately

[Link](#)



Tool (incubating): ArgoCD Hydrator



Rendered manifests pattern  Integrated



[Link](#)

  Renders and pushes manifests



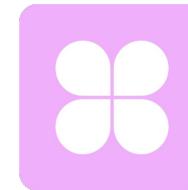


Dag Bjerre Andersen

From Denmark 

Infrastructure Engineer @ Doubble

Doubble is an app for double dating and meeting new people in groups



Ephemeral Clusters

How can we use ephemeral Kubernetes clusters to render your manifests changes directly on your pull requests?

Ephemeral Clusters

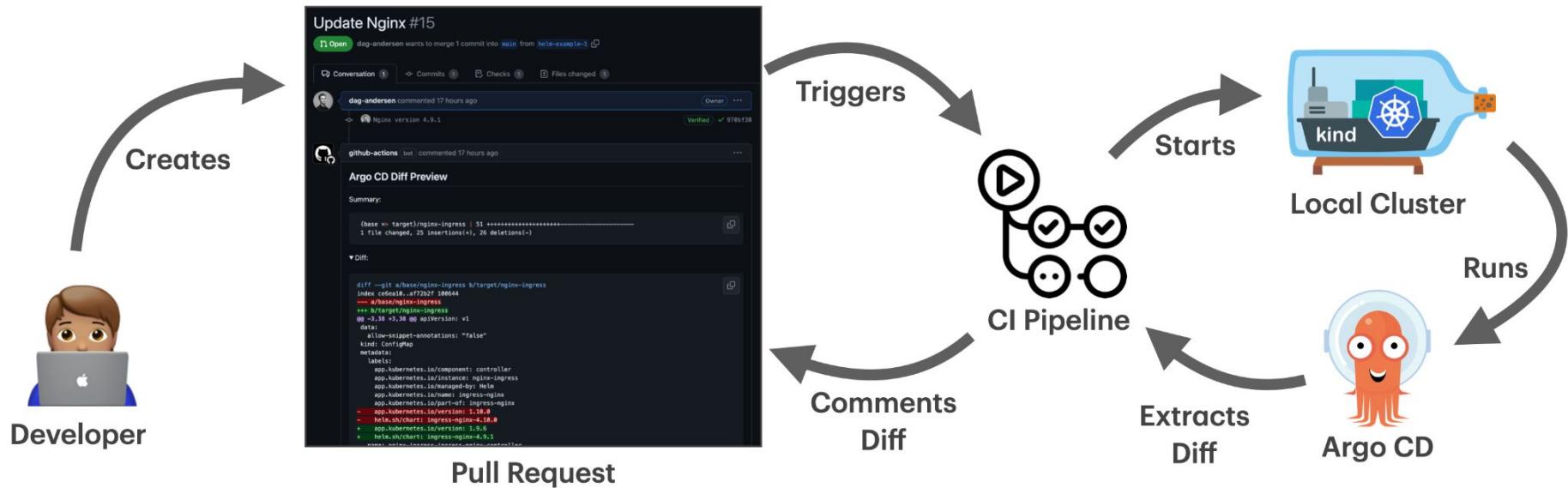


kind

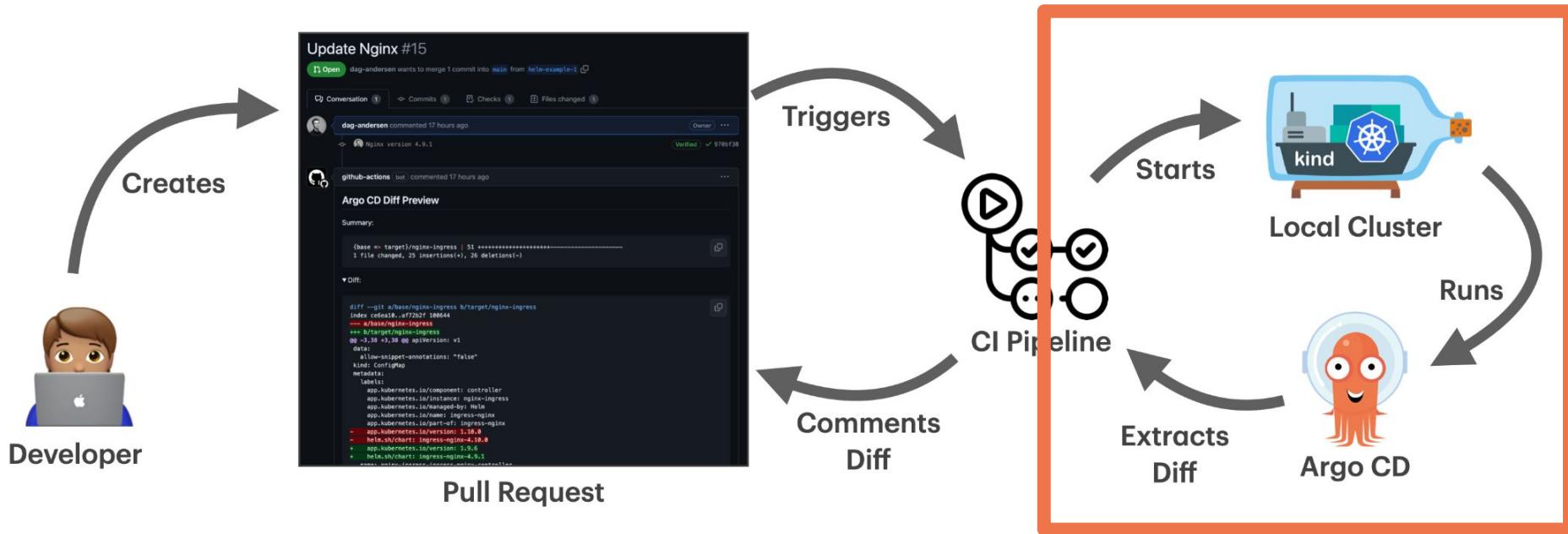


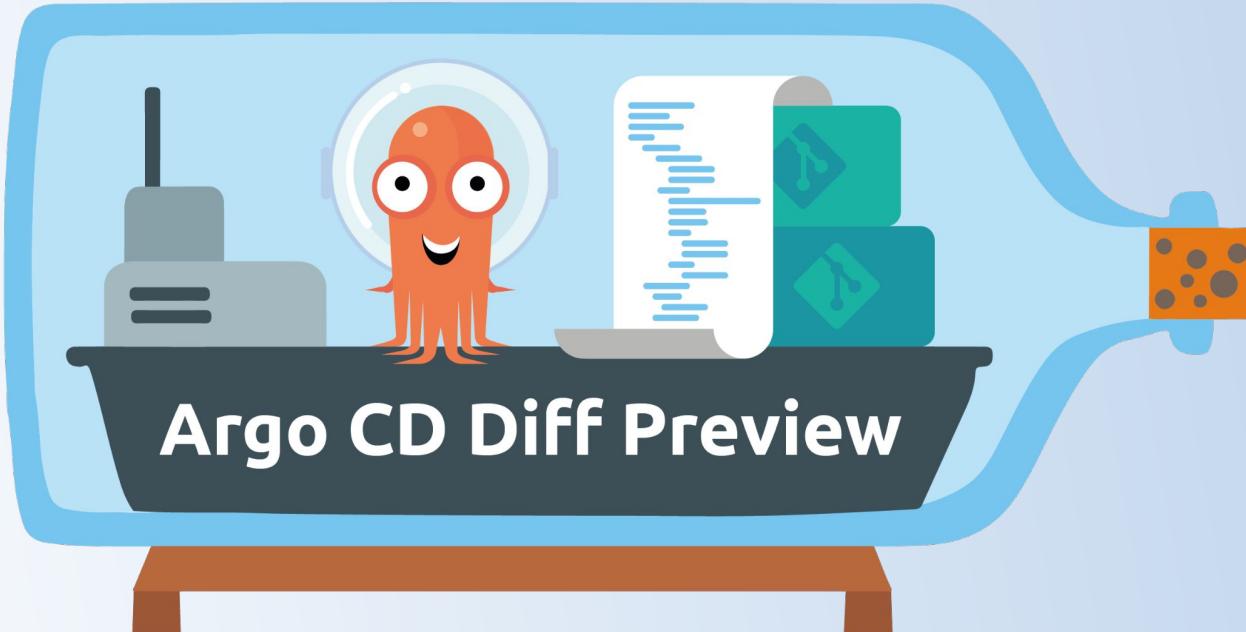
minikube

The Flow



The Flow







Demo

<https://github.com/dag-andersen/argocon-us-2024-demo>

Demo (in case wifi does not work) 1/3



```
v 2 ■■■■■ applications/my-app.yaml □ Viewed ...  
... ... @@ -1,18 +1,20 @@  
1 1 apiVersion: argoproj.io/v1alpha1  
2 2 kind: Application  
3 3 metadata:  
4 4   name: my-app  
5 5   namespace: argocd  
6 6 spec:  
7 7   project: default  
8 8   destination:  
9 9     name: in-cluster  
10 10    namespace: default  
11 11 sources:  
12 12     - repoURL: https://github.com/dag-andersen/argocon-demo  
13 13       ref: local-files  
14 14     - path: charts/myApp  
15 15       repoURL: https://github.com/dag-andersen/argocon-demo  
16 16     helm:  
17 17       valueFiles:  
18 18         - $local-files/values/values.yaml  
19 +     valuesObject:  
20 +       replicaCount: 5  
  
v 2 ■■■■■ values/values.yaml □ Viewed ...  
... ... @@ -1 +1 @@  
1 - fullnameOverride: super-app-name  
1 + fullnameOverride: argocon-demo
```

Demo (in case wifi does not work) 2/3



github-actions bot commented 3 weeks ago · edited

Argo CD Diff Preview

Summary:

```
{base => target}/my-app | 10 ++++++-----  
1 file changed, 5 insertions(+), 5 deletions(-)
```

▼ Diff:

```
diff --git base/my-app target/my-app  
index eb9e290..0e7966e 100644  
--- base/my-app  
+++ target/my-app  
@@ -2,21 +2,21 @@  
apiVersion: v1  
kind: Service  
metadata:  
  labels:  
    app.kubernetes.io/instance: my-app  
    app.kubernetes.io/managed-by: Helm  
    app.kubernetes.io/name: myApp  
    app.kubernetes.io/version: 1.16.0  
    argocd.argoproj.io/instance: my-app  
    helm.sh/chart: myApp-0.1.0  
-   name: super-app-name  
+   name: argocon-demo  
  namespace: default  
spec:  
  ports:
```

Demo (in case wifi does not work) 3/3



```
.github/workflows/generate-diff.yml

name: Argo CD Diff Preview

on:
  pull_request:
    branches:
      - main

jobs:
  build:
    runs-on: ubuntu-latest
    permissions:
      contents: read
      pull-requests: write

    steps:
      - uses: actions/checkout@v4
        with:
          path: pull-request

      - uses: actions/checkout@v4
        with:
          ref: main
          path: main

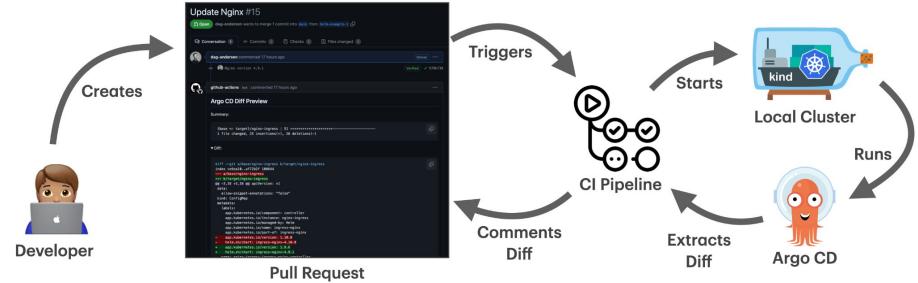
      - name: Generate Diff
        run:
          docker run \
            --network=host \
            -v /var/run/docker.sock:/var/run/docker.sock \
            -v ${pwd}/main:/base-branch \
            -v ${pwd}/pull-request:/target-branch \
            -v ${pwd}/output:/output \
            -e TARGET_BRANCH=${{ github.head_ref }} \
            -e REPO=${{ github.repository }} \
            dagandersen/argocd-diff-preview:v0.0.23

      - name: Post diff as comment
        run:
          gh pr comment ${{ github.event.number }} \
            --repo ${{ github.repository }} \
            --body-file output/diff.md
    env:
      GITHUB_TOKEN: ${{ secrets.GITHUB_TOKEN }}
```

How does it work? (1/2)



```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: something
spec:
  project: default
  syncPolicy:
    automated:
      prune: true
      selfHeal: true
  syncOptions:
    - ApplyOutOfSyncOnly=true
destination:
  name: https://whatever.com
  namespace: something
sources:
  - repoURL: https://github.com/dag-andersen/repo.git
    ref: local-files
    targetRevision: HEAD
  - chart: my-chart
    repoURL: helm-chart-registry.com
    targetRevision: x.x.x
    helm:
      releaseName: something
      valueFiles:
        - $local-files/whatever/values.yaml
```



How does it work? (1/2)

apiVersion: argoproj.io/v1alpha1

kind: Application

metadata:

 name: something

spec:

 imagePullSecrets:

 syncPolicy:

 automated:

 prune: true

 selfHeal: true

 syncOptions:

 - ApplyOutOfSyncOnly=true

 destination:

 name: https://whatever.com

 namespace: something

 sources:

 - repoURL: https://github.com/dag-andersen/repo.git

 ref: local-files

 targetRevision: HEAD

 - chart: my-chart

 repoURL: helm-chart-registry.com

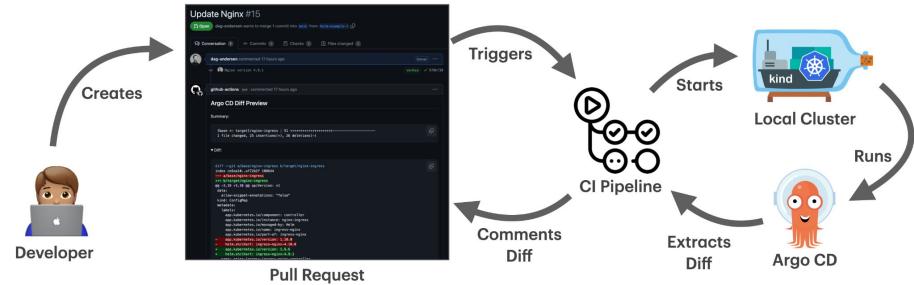
 targetRevision: x.x.x

 helm:

 releaseName: something

 valueFiles:

 - \$local-files/whatever/values.yaml



How does it work? (1/2)



apiVersion: argoproj.io/v1alpha1

kind: Application

metadata:

 name: something

spec:

 project: default

 syncPolicy:



destination:

 name: https://whatever.com

 namespace: something

sources:

- repoURL: https://github.com/dag-andersen/repo.git
 ref: local-files
 targetRevision: HEAD
- chart: my-chart
 repoURL: helm-chart-registry.com
 targetRevision: x.x.x
 helm:
 releaseName: something
 valueFiles:
 - \$local-files/whatever/values.yaml



How does it work? (1/2)



```
apiVersion: argoproj.io/v1alpha1
```

```
kind: Application
```

```
metadata:
```

```
  name: something
```

```
spec:
```

```
  project: default
```

```
  syncPolicy:
```



```
destination:
```

```
  name: https://whatever.com
```

```
  namespace: something
```

```
sources:
```

```
  - repoURL: https://github.com/dag-andersen/repo.git
```

```
    ref: local-files
```

```
    targetRevision: HEAD
```

```
  - chart: my-chart
```

```
    repoURL: helm-chart-registry.com
```

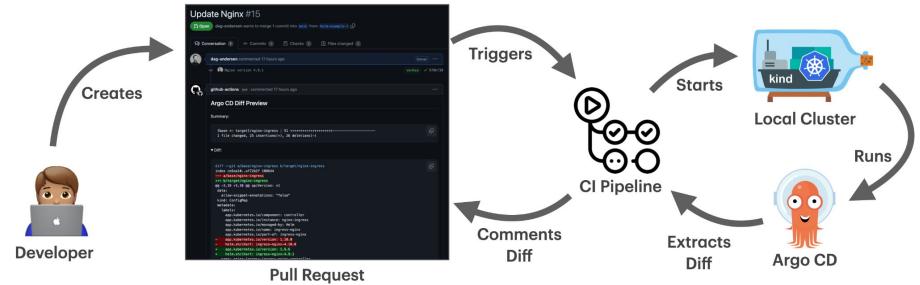
```
    targetRevision: x.x.x
```

```
    helm:
```

```
      releaseName: something
```

```
      valueFiles:
```

```
        - $local-files/whatever/values.yaml
```



How does it work? (1/2)

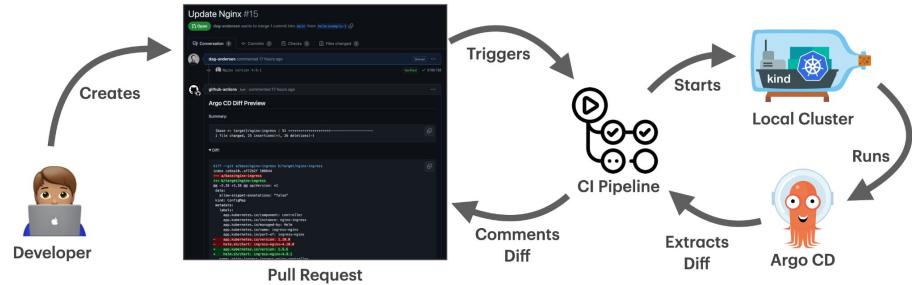
...

```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: something
spec:
  project: default
  syncPolicy:
```



```
destination:
  name: XXXXXX → "in-cluster" ↵
  namespace: something

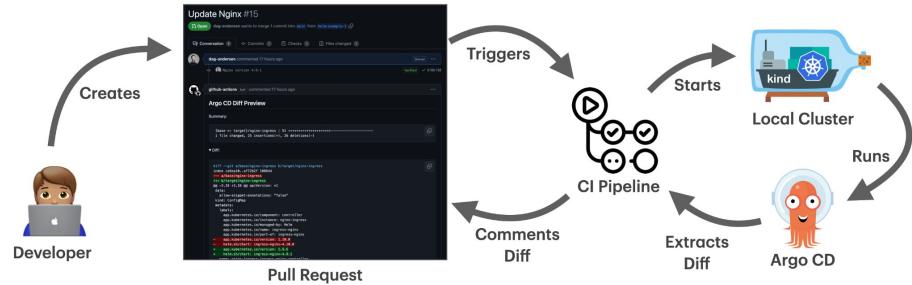
sources:
  - repoURL: https://github.com/dag-andersen/repo.git
    ref: local-files
    targetRevision: HEAD
  - chart: my-chart
    repoURL: helm-chart-registry.com
    targetRevision: x.x.x
    helm:
      releaseName: something
      valueFiles:
        - $local-files/whatever/values.yaml
```



How does it work? (1/2)

...

```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: something
spec:
  project: default
  syncPolicy:
    X
destination:
  name: XXXXXX → "in-cluster" ↵
  namespace: something
sources:
  - repoURL: https://github.com/dag-andersen/repo.git
    targetRevision: XXX → "<branch-name>" ↵
    chart: my-chart
    repoURL: helm-chart-registry.com
    targetRevision: x.x.x
    helm:
      releaseName: something
      valueFiles:
        - $local-files/whatever/values.yaml
```



How does it work? (2/2)



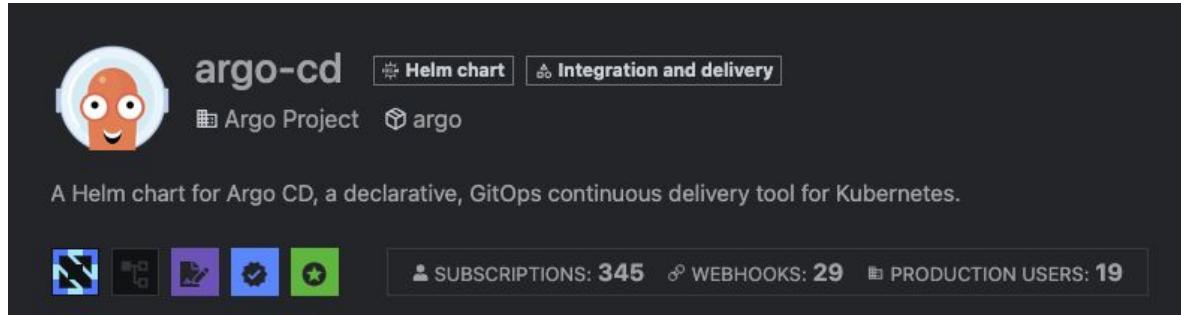
The screenshot shows the ArgoCD web interface. On the left is a sidebar with icons for applications, manifests, and logs. The main area has a header with "Applications" and a search bar containing "my-app". Below the header are five buttons: "DETAILS", "DIFF", "SYNC", "SYNC STATUS" (which is highlighted with a grey background), and "HISTORY AND RC". Under "APP HEALTH", there is a "Missing" status with a yellow emoji. Under "SYNC STATUS", the text "OutOfSync" is displayed in a large blue font, preceded by an orange icon with an upward arrow. This entire section is outlined with a red border. Below this, smaller text indicates "Auto sync is not enabled.", "Author: Dag Andersen -", and "Comment: something".

```
$ argocd app manifests <app> >> extracted.yaml
```

Custom Argo CD Installation and CMPs



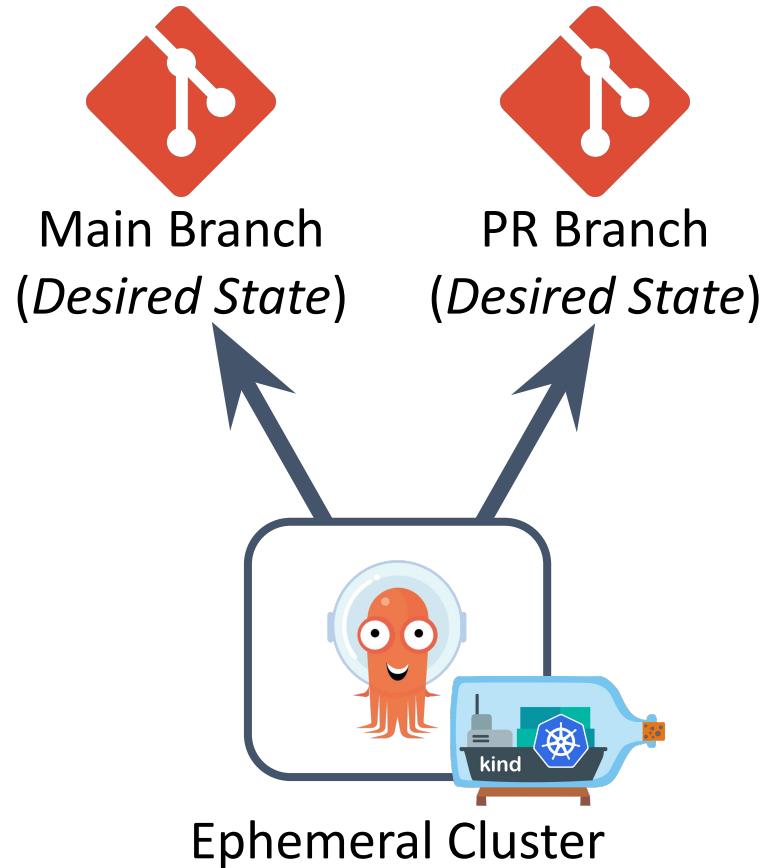
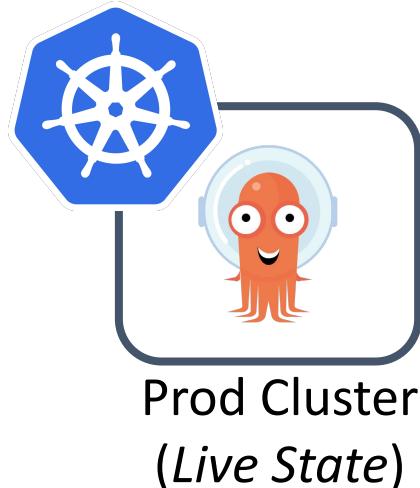
- Argo CD is installed through a Helm Chart
- You can edit any value you want
 - Match your live cluster
- You can install any Config Management Plugin that is installable from the Helm Chart



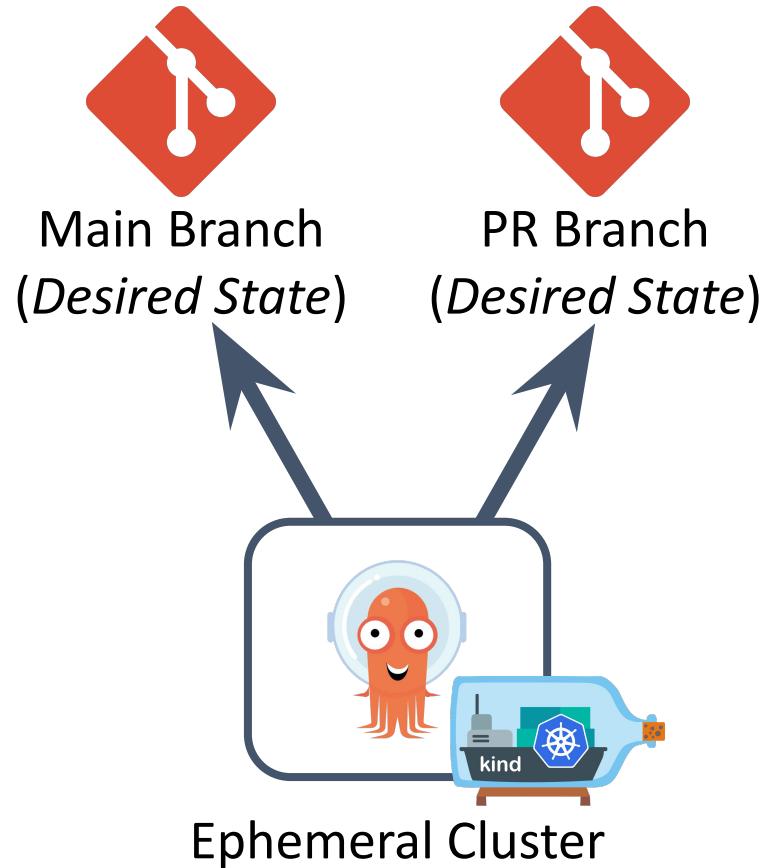
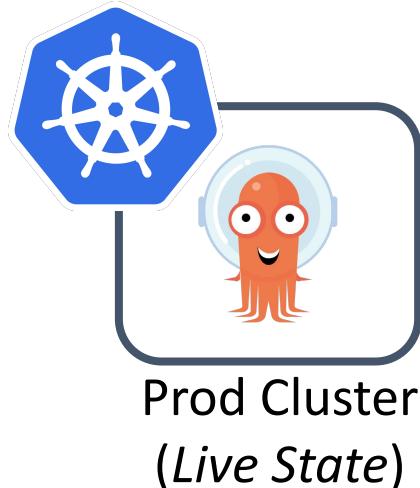
Desired state vs live state

When using ephemeral clusters

Comparing desired states only



Comparing desired states only



Faster feedback loop

We want to find issues before we merge

Faster feedback loop



creates a ↩

Faster feedback loop



ArgoCon
NORTH AMERICA

→

Applications /

DETAILS DIFF SYNC SYNC STATUS HISTORY AND ROLLBACK DELETE

APP HEALTH ? Healthy

SYNC STATUS ? Unknown failing-app-example

Auto sync is enabled.

... APP CONDITIONS

! 1 Error

The screenshot shows the ArgoCon UI for the 'my-app' application. On the left, there's a sidebar with icons for Applications, Workspaces, and Settings. The main area has a search bar with 'my-app'. Below it are several buttons: DETAILS, DIFF, SYNC, SYNC STATUS (which is highlighted), HISTORY AND ROLLBACK, and DELETE. Under these buttons, there are sections for APP HEALTH (Healthy), SYNC STATUS (Unknown, failing-app-example), and APP CONDITIONS (1 Error). A message at the bottom says 'Auto sync is enabled.'

Faster feedback loop



ArgoCon
NORTH AMERICA

The screenshot shows the ArgoCD application dashboard for the application "my-app". The top navigation bar includes a search bar with the query "my-app". Below the navigation are several action buttons: DETAILS, DIFF, SYNC, SYNC STATUS (which is highlighted), HISTORY AND ROLLBACK, and DELETE.

The main view displays three sections: APP HEALTH, SYNC STATUS, and APP CONDITIONS.

- APP HEALTH:** Shows a green heart icon and the status "Healthy".
- SYNC STATUS:** Shows the status as "Unknown" with the identifier "failing-app-example". A note below states "Auto sync is enabled."
- APP CONDITIONS:** Shows a red box containing a white exclamation mark and the text "1 Error".

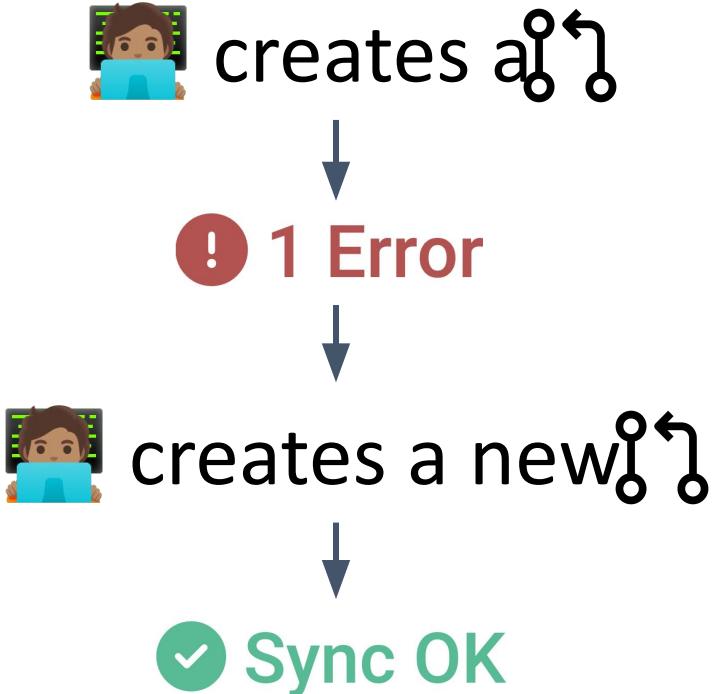
On the left side of the dashboard, there is a vertical sidebar with icons for Home, Applications, Workspaces, and Settings.

ComparisonError



```
Failed to load target state: failed to generate manifest for source 2 of 2: rpc error: code = Unknown desc =
`helm template . --name-template my-app --namespace default --kube-version 1.31 --values <path to
cached source>/examples/some/wrong/path/values.yaml <api versions removed> --include-crds` failed
exit status 1: Error: open <path to cached source>/examples/some/wrong/path/values.yaml: no such file
or directory
```

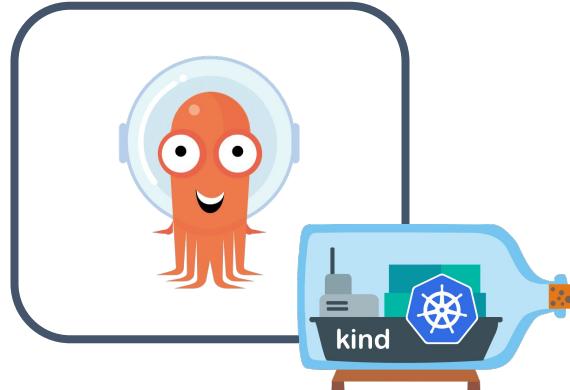
Faster feedback loop



Faster feedback loop



! 1 Error



Ephemeral Cluster

Faster feedback loop



```
🏃 Installing Argo CD Helm Chart version: 'latest'  
🏃 Waiting for Argo CD to start...  
🏃 Argo CD is now available  
🏃 Logging in to Argo CD through CLI...  
🏃 Argo CD installed successfully  
🌐 Getting resources from base-branch  
⌚ Waiting for 5 out of 5 applications to become 'OutOfSync'. Retrying in 5 seconds. Timeout in 180 seconds...  
🌐 Got all resources from 5 applications for base  
🚤 Removing applications  
🚤 Removed applications successfully  
🌐 Getting resources from target-branch  
⌚ Waiting for 5 out of 5 applications to become 'OutOfSync'. Retrying in 5 seconds. Timeout in 180 seconds...  
✗ Failed to process application: my-app with error:  
Failed to load target state: failed to generate manifest for source 2 of 2: rpc error: code = Unknown desc = `helm template .  
--name-template my-app --namespace default --kube-version 1.31 --values <path to cached source>/examples/some/wrong/path/values.yaml  
<api versions removed> --include-crds` failed exit status 1: Error: open <path to cached source>/examples/some/wrong/path/values.  
yaml: no such file or directory  
Error: "Failed to process applications"
```



Limitations

Things to keep in mind...

False sense of security



Some issues happen at run time (or at resource creation time)

False sense of security



Some issues happen at run time (or at resource creation time)

Examples of things that can break:

- Pods being rejected because of: `securityContext.runAsNonRoot: true`

False sense of security



Some issues happen at run time (or at resource creation time)

Examples of things that can break:

- Pods being rejected because of: `securityContext.runAsNonRoot: true`
- Missing `CustomResourceDefinitions` in your destination cluster

<p>SYNC STATUS ⓘ</p> <p>⚠️ OutOfSync from main (7fc4949) and (1) more</p> <p>Auto sync is not enabled.</p> <p>Author: Dag Andersen -</p> <p>Comment: something</p>	<p>LAST SYNC ⓘ</p> <p>✖️ Sync failed to 7fc4949 and (1) more</p> <p>Failed 2 minutes ago (Wed Oct 30 2024 13:52:32 GMT+0100)</p> <p>Author: Dag Andersen -</p> <p>Comment: something</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Speed



- Spinning up a local Kubernetes cluster and installing Argo CD on it every single run takes time
 - It takes around 70 seconds
- The full PR pipeline may take 2+ minutes
 - Pulling code x2
 - Pulling the docker image
 - Running the tool
- Speed depends on how many applications you are rendering

GitHub Issues



ArgoCon
NORTH AMERICA

	Author ▾
3 Open	✓ 13 Closed
<input type="checkbox"/> (+) Support multiple sources <small>should-work</small>	#58 by rikez was closed 16 hours ago
<input type="checkbox"/> (+) Support argocd.argoproj.io/manifest-generate-paths <small>enhancement good first issue</small>	#57 opened yesterday by gozer
<input type="checkbox"/> (+) Only asset for linux arm64 was released at v0.0.22	#55 by suzuki-shunsuke was closed last week
<input type="checkbox"/> (+) helm dependency build failing with empty index.yaml file <small>bug</small>	#48 opened on Oct 2 by piljaechae
<input type="checkbox"/> (+) Rendering Issue Could not resolve hostname github.com	#44 by sachinmalanki was closed last month
<input type="checkbox"/> (+) Feature Add label selectors for filtering what applications to render <small>enhancement</small>	#43 by dag-andersen was closed on Sep 20
<input type="checkbox"/> (+) Change diff > Github Comment Limit	#42 by seanturner026 was closed on Sep 16
<input type="checkbox"/> (+) Is this project meant to work for App-of-apps pattern?	#41 by davidfrickert was closed on Sep 4
<input type="checkbox"/> (+) Support for ArgoCD config management plugins <small>enhancement should-work</small>	#40 opened on Sep 1 by davidfrickert
<input type="checkbox"/> (+) Can the destination patching be optional?	#38 by aokomorowski was closed on Aug 13
<input type="checkbox"/> (+) Kustomize op Patches cause a Panic	#35 by seanturner026 was closed on Aug 6
<input type="checkbox"/> (+) TargetRevision field is patched even if the source type is set to Helm <small>bug</small>	#33 by aokomorowski was closed on Aug 1
<input type="checkbox"/> (+) error: Error from server (NotFound): secrets "argocd-initial-admin-secret" not found	#32 by dag-andersen was closed on Aug 6
<input type="checkbox"/> (+) self hosted - adding known hosts via config map <small>question</small>	#30 by bainss was closed 18 hours ago
<input type="checkbox"/> (+) Templated values are not evaluated in ApplicationSets before executing helm template	#29 by aokomorowski was closed on Aug 1
<input type="checkbox"/> (+) No changes found <small>bug</small>	#27 by seanturner026 was closed on Jun 17

Adoption

Who uses `argocd-diff-preview`?

Companies using argocd-diff-preview



400F

New Day

Summarize main points

What did we learn?

Summary



Main benefits of using *ephemeral clusters*

- Runs in complete isolation
 - Great for security
- Runs in parallel
 - No queues, No locks, No webhooks
- Enables comparing desired states only
 - Out-of-sync apps are not a problem
 - Can even be run locally

Main limitations

- Spinning up a local cluster and installing Argo CD is slow
- Can give a false sense of security

Main benefits of using *specifically* `argocd-diff-preview`

- Easy to set up
- Not opinionated
 - It only compares branches



Main limitations

- Does not work well when the Argo CD configuration is spread across multiple repositories
 - We are currently working on improving this

Thank you!



If you have any questions, please feel free to reach out to us after the talk, on LinkedIn, or on CNCF Slack



Dag Bjerre Andersen
LinkedIn

<https://www.linkedin.com/in/dagbjerreandersen/>



argocd-diff-preview
GitHub

<https://github.com/dag-andersen/argocd-diff-preview>



Regina Voloshin
LinkedIn

<https://www.linkedin.com/in/regina-voloshin-09b9841/>