Cloud Native CI/CD with Tekton

2023-10-26
Mansun Kuo

Table of contents

Preface

Tekton in a Nutshell

Tips and Tricks

Key Takeaways

Preface

Cloud Native

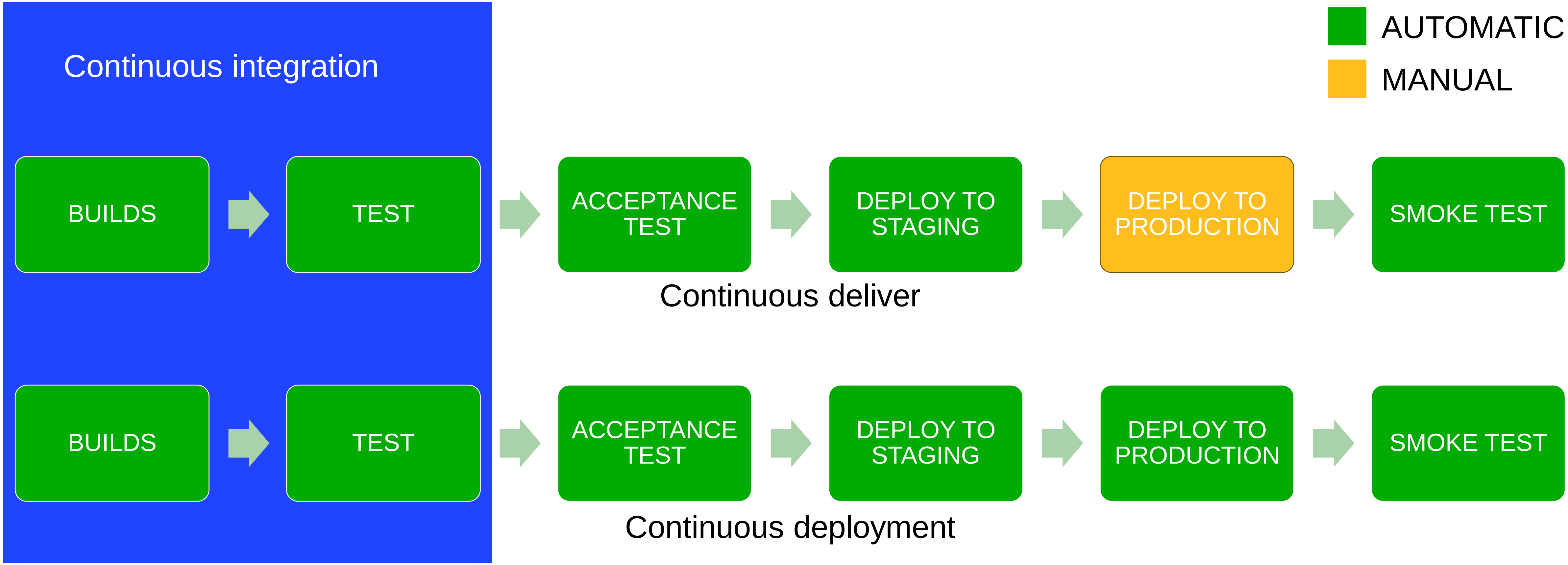
The software approach for modern applications in cloud computing environments.

- Architecture
  - Container
  - Immutable infrastructure
  - Microservices
  - Declarative APIs
  - Service mesh
- Development
  - CI/CD
  - DevOps
  - Serverless

https://aws.amazon.com/what-is/cloud-native/
https://www.cncf.io/wp-content/uploads/2020/08/cncf_ambassador-768x628-1.png

CI/CD

A set of practices that aim to automate the process of developing, testing, and delivering software applications



🟩 AUTOMATIC

🟨 MANUAL

Continuous integration

BUILDS → TEST → ACCEPTANCE TEST → DEPLOY TO STAGING → DEPLOY TO PRODUCTION → SMOKE TEST

Continuous deliver

BUILDS → TEST → ACCEPTANCE TEST → DEPLOY TO STAGING → DEPLOY TO PRODUCTION → SMOKE TEST

Continuous deployment

https://www.atlassian.com/continuous-delivery/principles/continuous-integration-vs-delivery-vs-deployment

A True Story

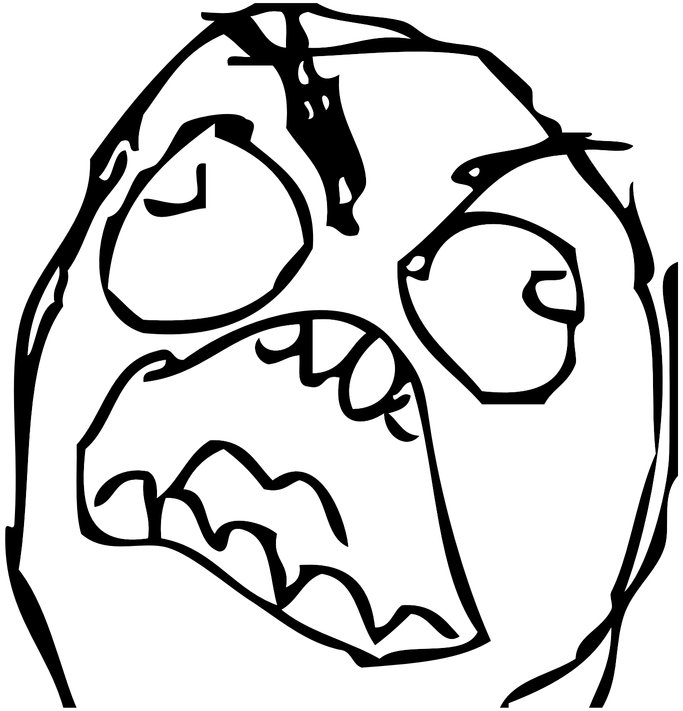
My ex-colleague reconnected with me before DevOpsDays

Jenkins

Azure Pipelines

Github Actions

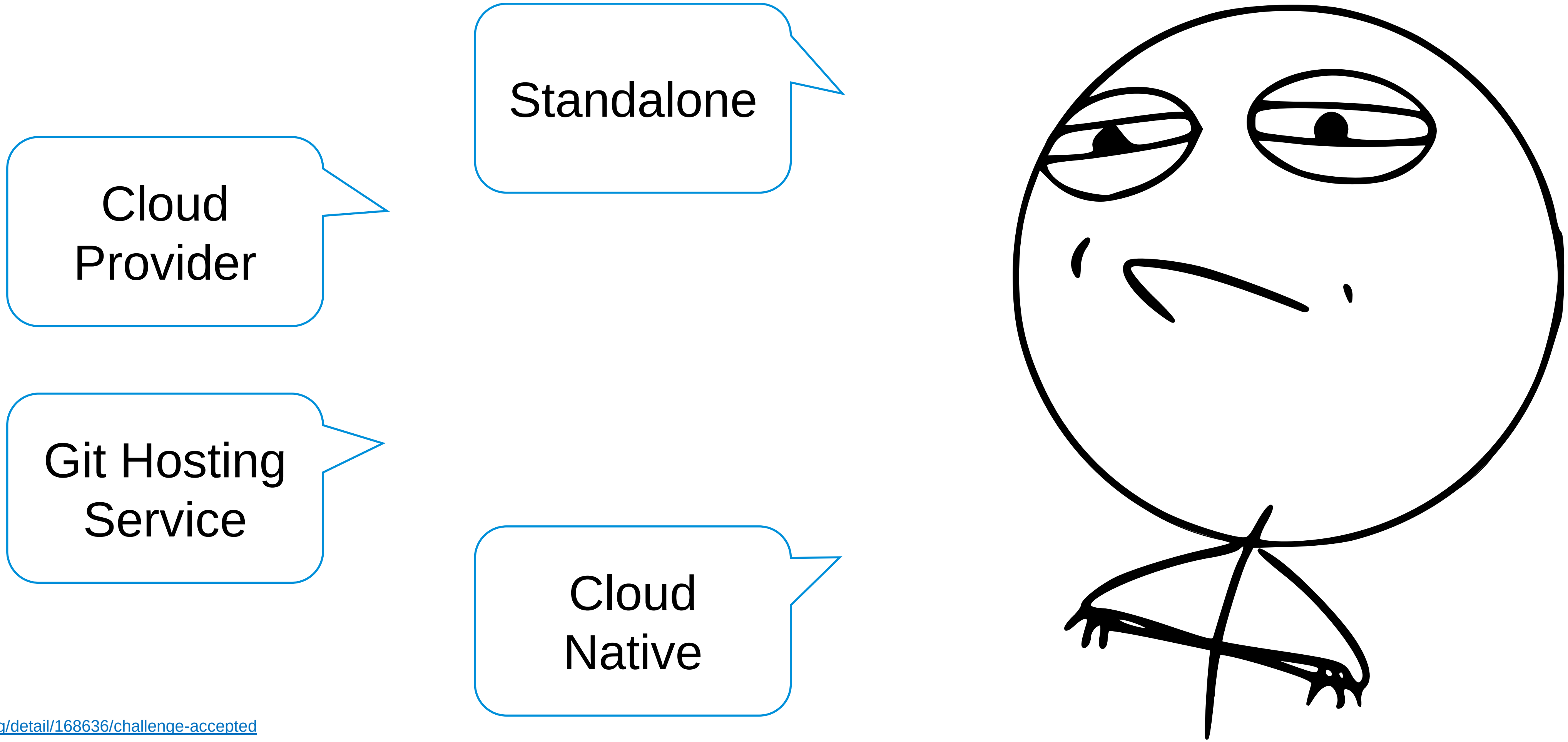
Tekton



https://openclipart.org/detail/142225/rage-guy

A True Story

They are exactly different types of CI/CD tools



Standalone

Cloud Provider

Git Hosting Service

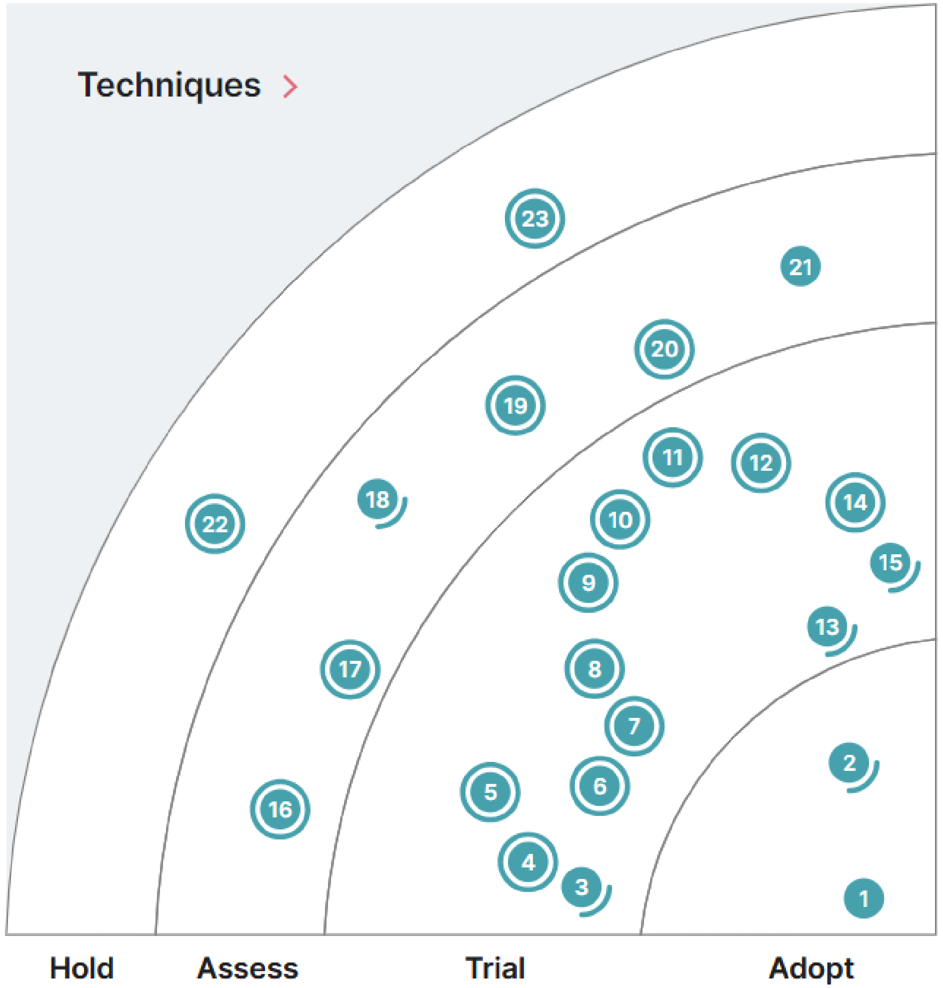
Cloud Native

https://openclipart.org/detail/168636/challenge-accepted

Zero Trust Security for CI/CD

Trail in Thoughtworks Technology Radar, Techniques (Sep. 2023)

- Pipeline doesn’t direct access to secrets
- Limit access, no “god user accounts”
- Ephemeral runners, don’t reuse them
- Keep agents and runners updated
- Monitor CI/CD systems



https://www.thoughtworks.com/radar/techniques/zero-trust-security-for-ci-cd
https://www.thoughtworks.com/radar

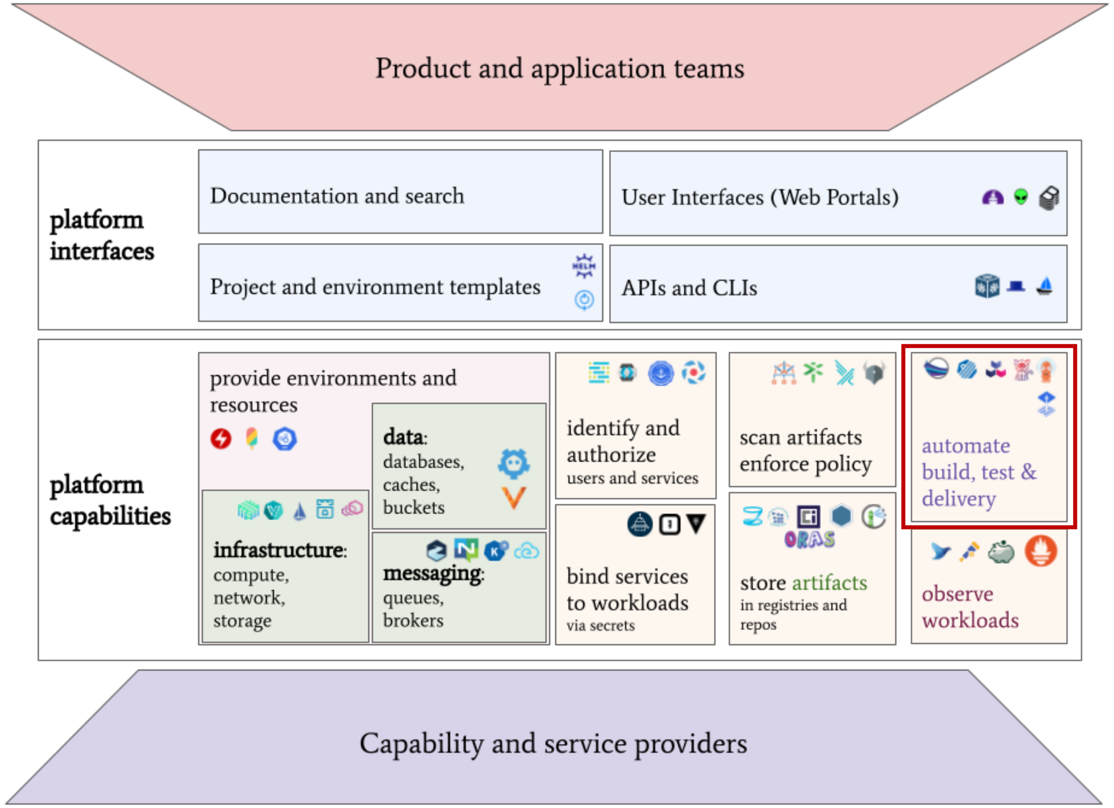
The Rise of Platform Engineering

"A digital platform is a foundation of self-service APIs, tools, services, knowledge and support which are arranged as a compelling internal product."

Martin Fowler and Evan Bottcher

*"A **platform** aggregates capabilities to serve developers and operators in development and delivery of products, services and apps."*

CNCF Platforms White Paper



Product and application teams

platform interfaces

Documentation and search

User Interfaces (Web Portals)

Project and environment templates

APIs and CLIs

platform capabilities

provide environments and resources

data: databases, caches, buckets

infrastructure: compute, network, storage

messaging: queues, brokers

identify and authorize users and services

bind services to workloads via secrets

scan artifacts enforce policy

store artifacts in registries and repos

automate build, test & delivery

observe workloads

Capability and service providers

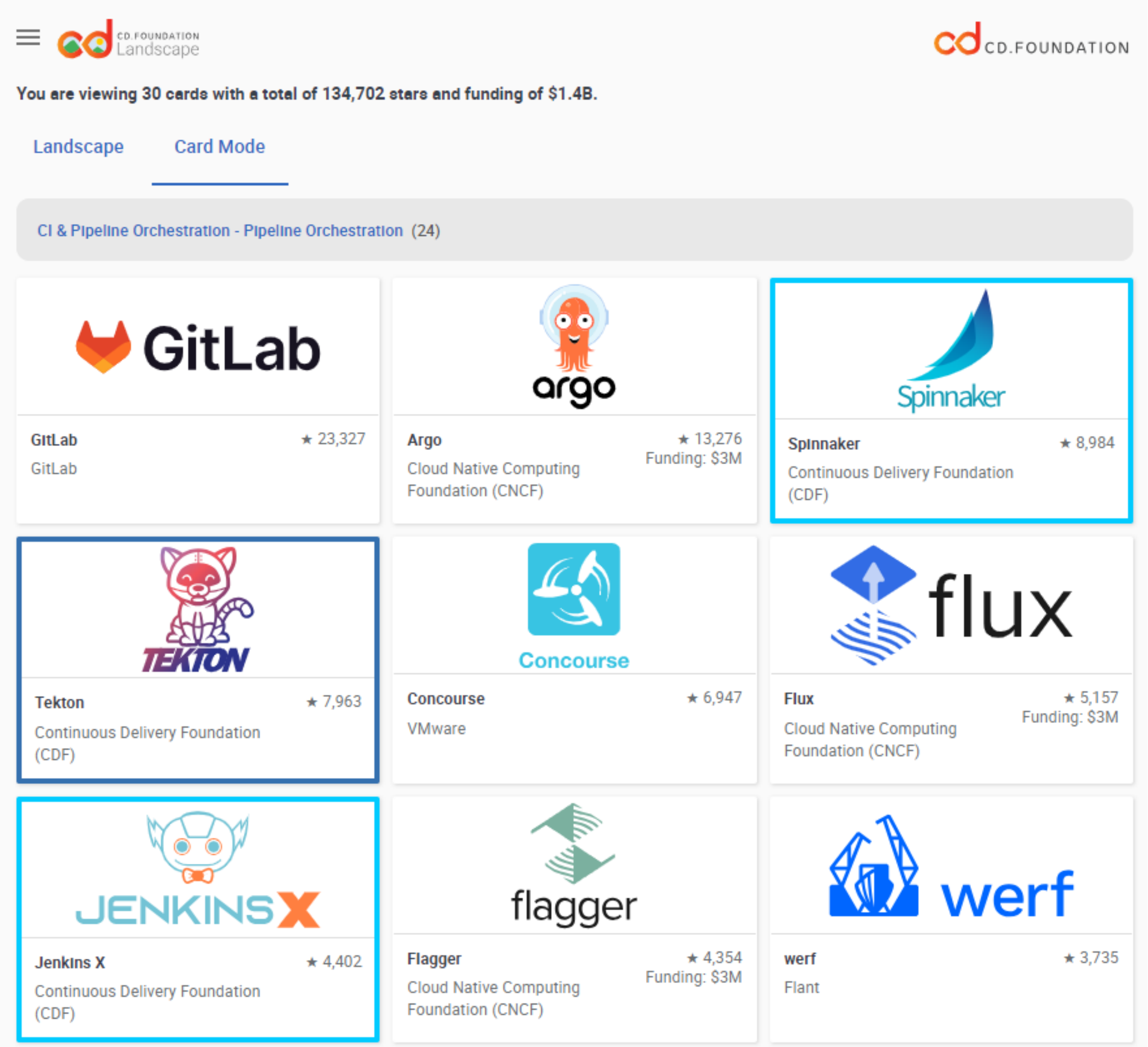
https://martinfowler.com/articles/talk-about-platforms.html
https://tag-app-delivery.cncf.io/whitepapers/platforms/

Tekton in a Nutshell

What is Tekton

- A cloud native solution for CI/CD
- Spun-off from Knative
- K8s custom resource of building blocks
- Built-in best practices
  - Scalable, serverless, cloud-native
- Community
  - Graduate from the CD Foundation
  - An official product or recommended solution from Google, Red Hat and IBM
- Supply chain security

https://landscape.cd.foundation/card-mode?category=ci-pipeline-orchestration&grouping=category&sort=stars



You are viewing 30 cards with a total of 134,702 stars and funding of $1.4B.

CI & Pipeline Orchestration - Pipeline Orchestration (24)

GitLab ★ 23,327
GitLab

Argo ★ 13,276
Cloud Native Computing Foundation (CNCF)
Funding: $3M

Spinnaker ★ 8,984
Continuous Delivery Foundation (CDF)

Tekton ★ 7,963
Continuous Delivery Foundation (CDF)

Concourse ★ 6,947
VMware

Flux ★ 5,157
Cloud Native Computing Foundation (CNCF)
Funding: $3M

Jenkins X ★ 4,402
Continuous Delivery Foundation (CDF)

Flagger ★ 4,354
Cloud Native Computing Foundation (CNCF)
Funding: $3M

werf ★ 3,735
Flant

Who are the Potential User of Tekton

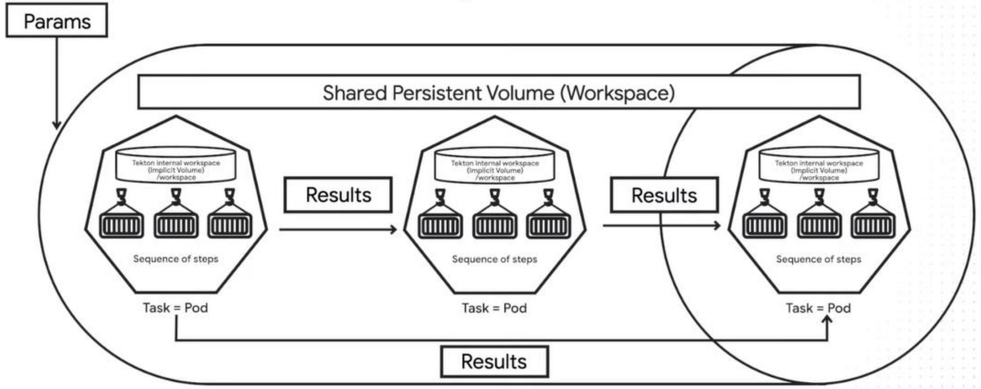
- You are looking for a cloud-native solution across multiple public/private cloud
- CI/CD infrastructure as a service is not available for you
- Your organization already have products with built-in Tekton pipeline
  - OpenShift
  - IBM Cloud
- You are going to build a CI/CD platform

https://cd.foundation/wp-content/uploads/sites/78/2019/02/tekton-color.svg
https://user-images.githubusercontent.com/727396/84170826-eb3bbe00-aa2e-11ea-8d59-122bfe38cf3f.png
https://user-images.githubusercontent.com/12814972/73849604-22505780-4822-11ea-9fb0-a92fa185ee2a.png
https://tekton.dev/docs/dashboard/tekton-dashboard-color.svg

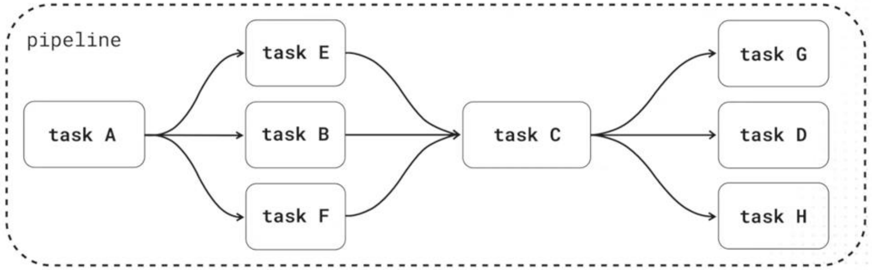
Tekton Pipeline

- Step
  - Smallest unit to run command or script
  - A container
- Task:
  - A sequence of steps
  - A pod with entrypoint override
  - An abstraction of reusable component
- Pipeline:
  - A Directed Acyclic Graph of Tasks
  - Shared data between tasks through results and workspace(persistent Volume)
  - Use syntax like retries, when and finally to handle workflow
- Workspace: k8s volume
- Results: k8s termination message

Pipeline


Params
Shared Persistent Volume (Workspace)
Tekton internal workspace (Implicit Volume) /workspace
Sequence of steps
Task = Pod
Results
Tekton internal workspace (Implicit Volume) /workspace
Sequence of steps
Task = Pod
Results
Tekton internal workspace (Implicit Volume) /workspace
Sequence of steps
Task = Pod
Results

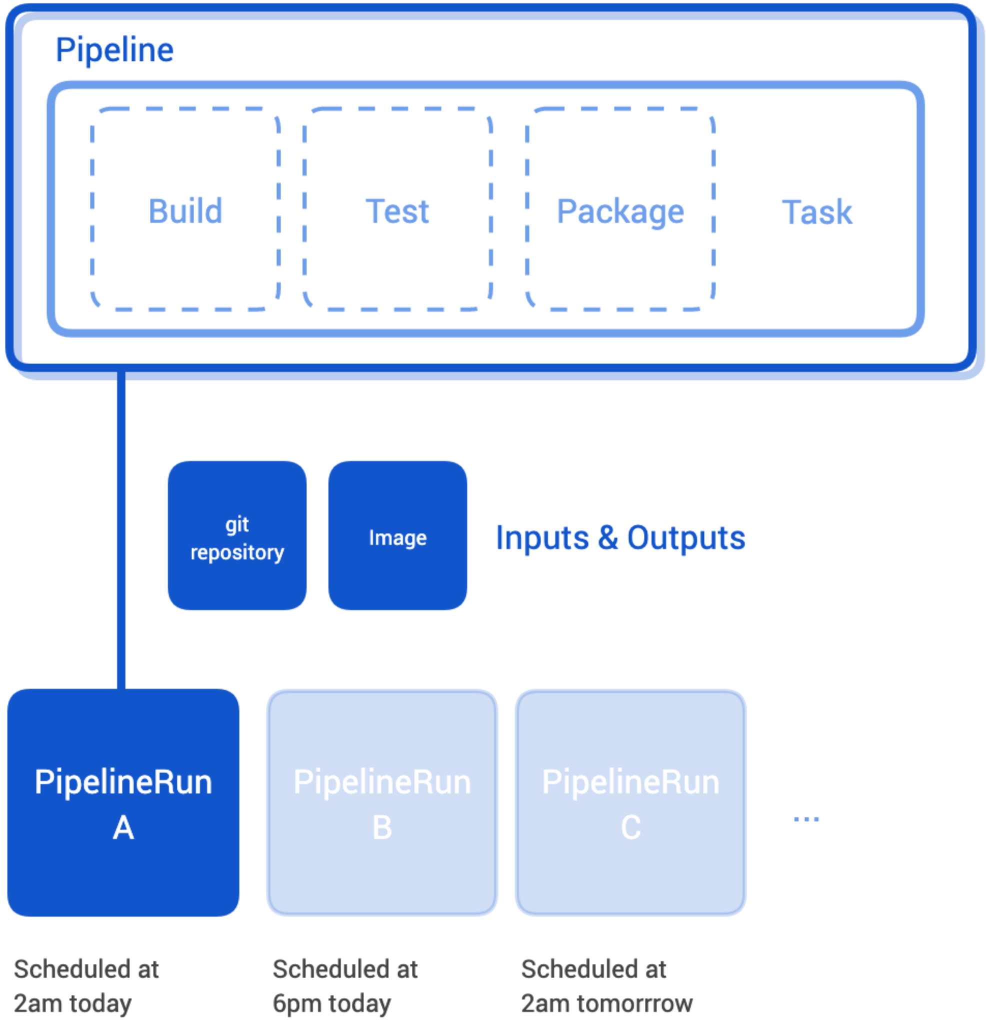
Pipeline as a Directed Acyclic Graph



Snapshotted from https://www.youtube.com/watch?v=pW606eBa7og

TaskRuns and PipelineRuns

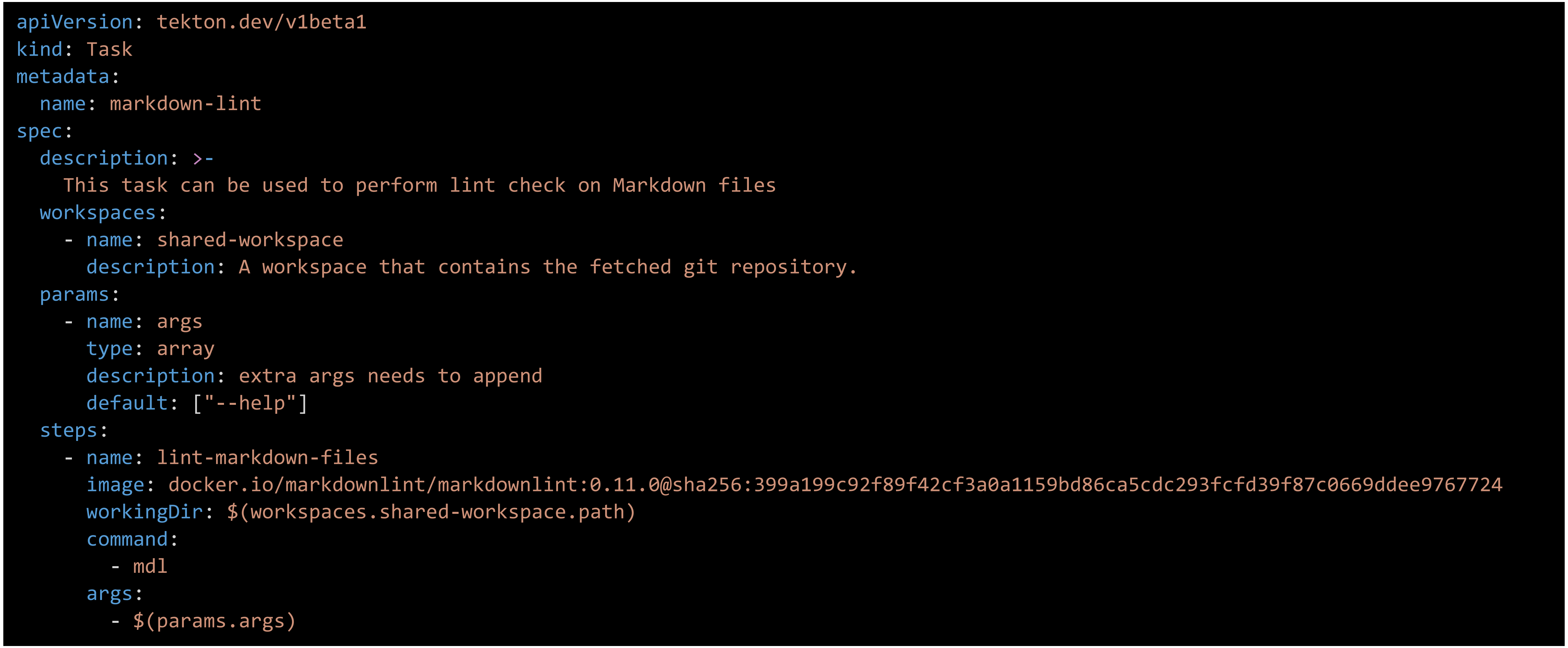
- A specific execution of a task/pipeline
- Connect resources with parameters
- Created manually or with a Trigger



https://tekton.dev/docs/concepts/concept-runs.png

Task

This task using an image to lint Markdown with args as its parameter

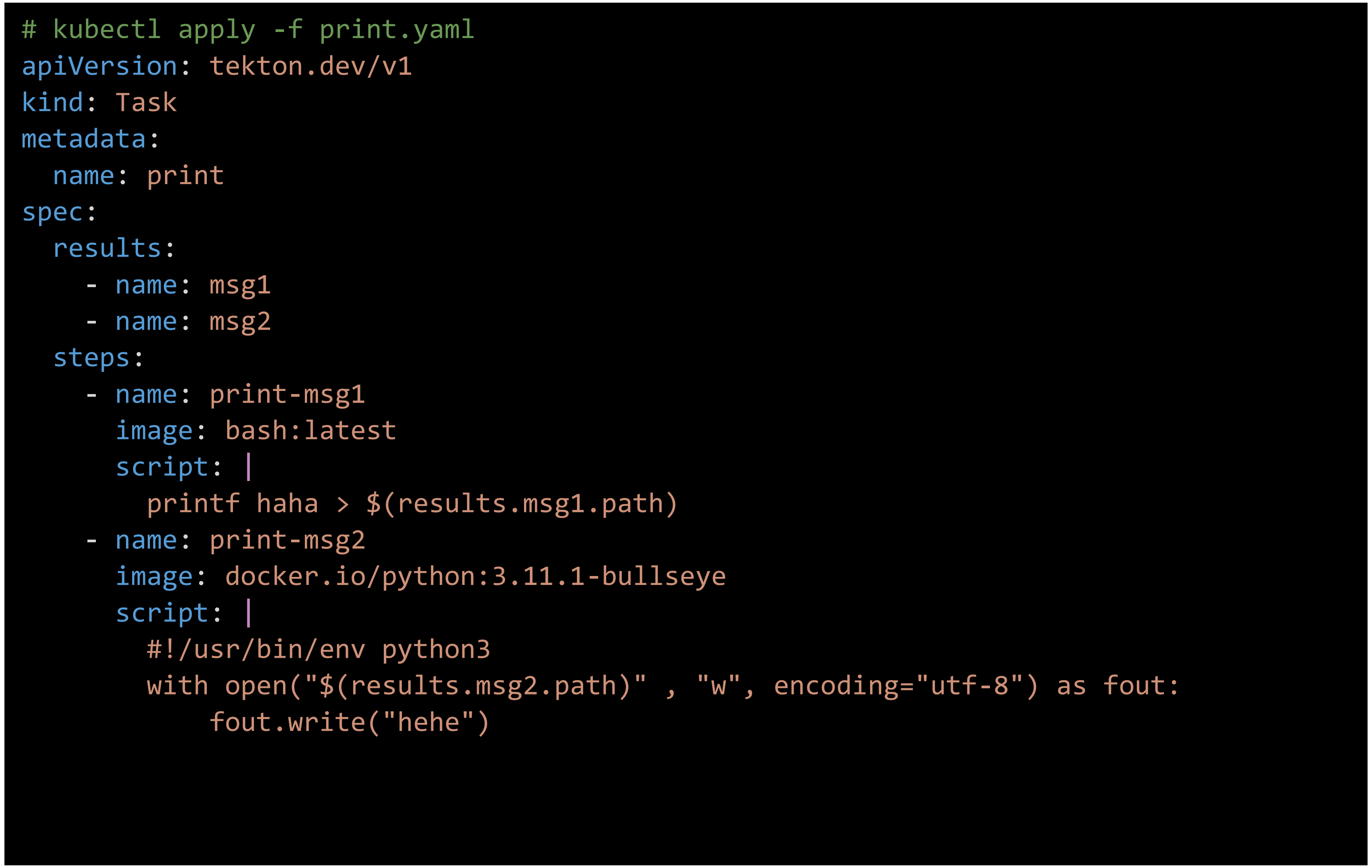


```yaml
apiVersion: tekton.dev/v1beta1
kind: Task
metadata:
  name: markdown-lint
spec:
  description: >-
    This task can be used to perform lint check on Markdown files
  workspaces:
    - name: shared-workspace
      description: A workspace that contains the fetched git repository.
  params:
    - name: args
      type: array
      description: extra args needs to append
      default: ["--help"]
  steps:
    - name: lint-markdown-files
      image: docker.io/markdownlint/markdownlint:0.11.0@sha256:399a199c92f89f42cf3a0a1159bd86ca5cdc293fcfd39f87c0669ddee9767724
      workingDir: $(workspaces.shared-workspace.path)
      command:
        - mdl
      args:
        - $(params.args)
```

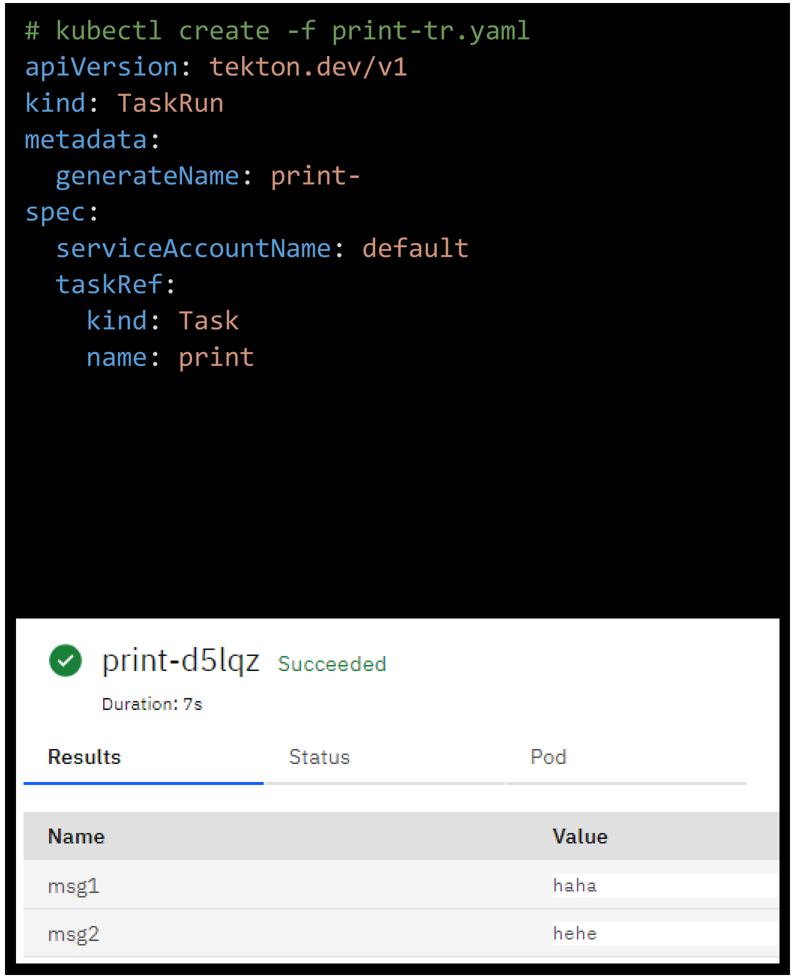
https://hub.tekton.dev/tekton/task/markdown-lint

Task with Results

Emitting results is just writing something into a file



```yaml
# kubectl apply -f print.yaml
apiVersion: tekton.dev/v1
kind: Task
metadata:
  name: print
spec:
  results:
    - name: msg1
    - name: msg2
  steps:
    - name: print-msg1
      image: bash:latest
      script: |
        printf haha > $(results.msg1.path)
    - name: print-msg2
      image: docker.io/python:3.11.1-bullseye
      script: |
        #!/usr/bin/env python3
        with open("$(results.msg2.path)" , "w", encoding="utf-8") as fout:
            fout.write("hehe")
```



```yaml
# kubectl create -f print-tr.yaml
apiVersion: tekton.dev/v1
kind: TaskRun
metadata:
  generateName: print-
spec:
  serviceAccountName: default
  taskRef:
    kind: Task
    name: print
```

print-d5lqz Succeeded

Duration: 7s

Name	Value
msg1	haha
msg2	hehe

https://tekton.dev/docs/pipelines/tasks/#emitting-results

Pipeline

An example that guard manual-approval, build-image and deploy-image with `merge` and send slack finally

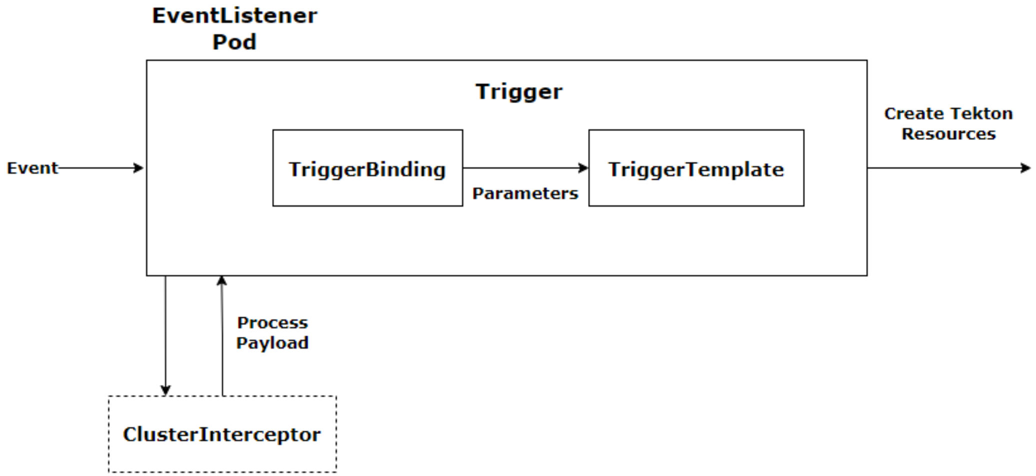
```yaml
#...
tasks:
- name: manual-approval
  runAfter:
    - tests
  when:
    - input: $(params.git-action)
      operator: in
      values:
        - merge
  taskRef:
    name: manual-approval

- name: build-image
  when:
    - input: $(params.git-action)
      operator: in
      values:
        - merge
  runAfter:
    - manual-approval
  taskRef:
    name: build-image
```

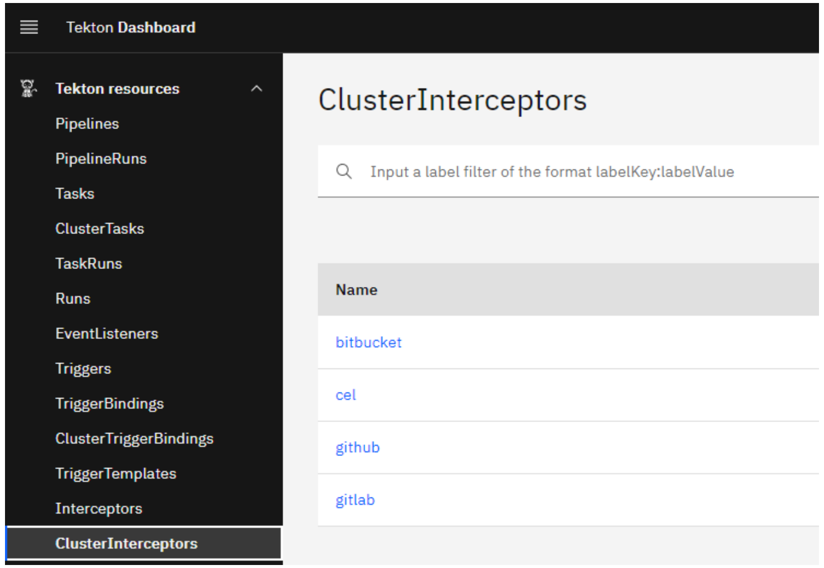
```yaml
- name: deploy-image
  when:
    - input: $(params.git-action)
      operator: in
      values:
        - merge
  runAfter:
    - build-image
  retries: 3
  taskRef:
    name: deploy-image

finally:
- name: slack-msg
  params:
    - name: approver
      value: $(tasks.manual-approval.results.approver)
  taskRef:
    name: slack-msg
```

https://tekton.dev/docs/pipelines/pipelines/

Tekton Trigger and EventListener

- Event Listener
  - Listens to events and specifies triggers
- Interceptor
  - Payload filtering
  - Verification
  - Transformation
- Trigger Binding
  - Uses JSONPath to extracts the event information from the event payload
- Trigger Template
  - Provides a blueprint for creating a TaskRun or a PipelineRun





ClusterInterceptors

Input a label filter of the format labelKey:labelValue

Name
bitbucket
cel
github
gitlab

https://tekton.dev/docs/getting-started/triggers/

EventListener

An example using bitbucket interceptor with k8s secret and Bitbucket eventType

```yaml
apiVersion: triggers.tekton.dev/v1beta1
kind: EventListener
metadata:
  name: bitbucket-server-listener
spec:
  serviceAccountName: tekton-triggers-example-sa
  triggers:
    - name: bitbucket-server-triggers
      interceptors:
        - ref:
            name: "bitbucket"
          params:
            - name: secretRef
              value:
                secretName: bitbucket-server-secret
                secretKey: secretToken
            - name: eventTypes
              value:
                - repo:refs_changed
      bindings:
        - ref: bitbucket-server-binding
      template:
        ref: bitbucket-server-template
```

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: bitbucket-server-secret
type: Opaque
stringData:
  secretToken: "1234567"
```

https://github.com/tektoncd/triggers/blob/main/examples/v1beta1/bitbucket-server/bitbucket-listener.yaml
https://github.com/tektoncd/triggers/blob/main/examples/v1beta1/bitbucket-server/secret.yaml

TriggerBinding

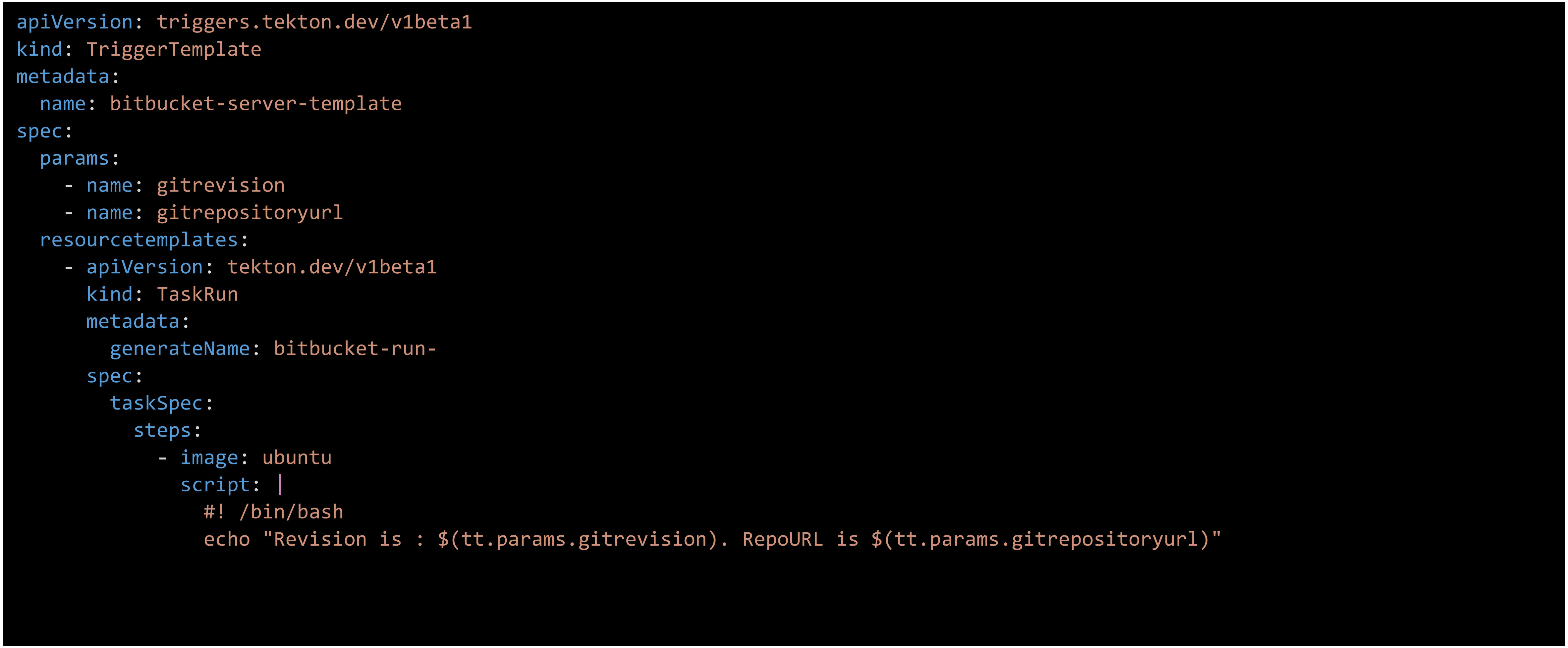
An example using $(body) and JSONPath to parse request body

```
# curl -v \
# -H 'X-Event-Key: repo:refs_changed' \
# -H 'X-Hub-Signature: sha1=b3fdaf5d1a47e57527764a233659c650a11abdd8' \
# -d '{"repository": {"links": {"clone": [{"href": "http://localhost:7990/scm/~test/helloworld.git", "name": "http"}, {"href":
"ssh://git@localhost:7999/~test/helloworld.git", "name": "ssh"}]}}, "changes": [{"ref": {"displayId": "main"}}]}' \
# http://localhost:8080

apiVersion: triggers.tekton.dev/v1beta1
kind: TriggerBinding
metadata:
  name: bitbucket-server-binding
spec:
  params:
    - name: gitrevision
      value: $(body.changes[0].ref.displayId)
    - name: gitrepositoryurl
      value: $(body.repository.links.clone[?(@.name=="ssh")].href)
```

https://github.com/tektoncd/triggers/blob/main/examples/v1beta1/bitbucket-server/triggerbinding.yaml

TriggerTemplate

An example using `$(tt.params)` to access params parsed from TriggerBinding

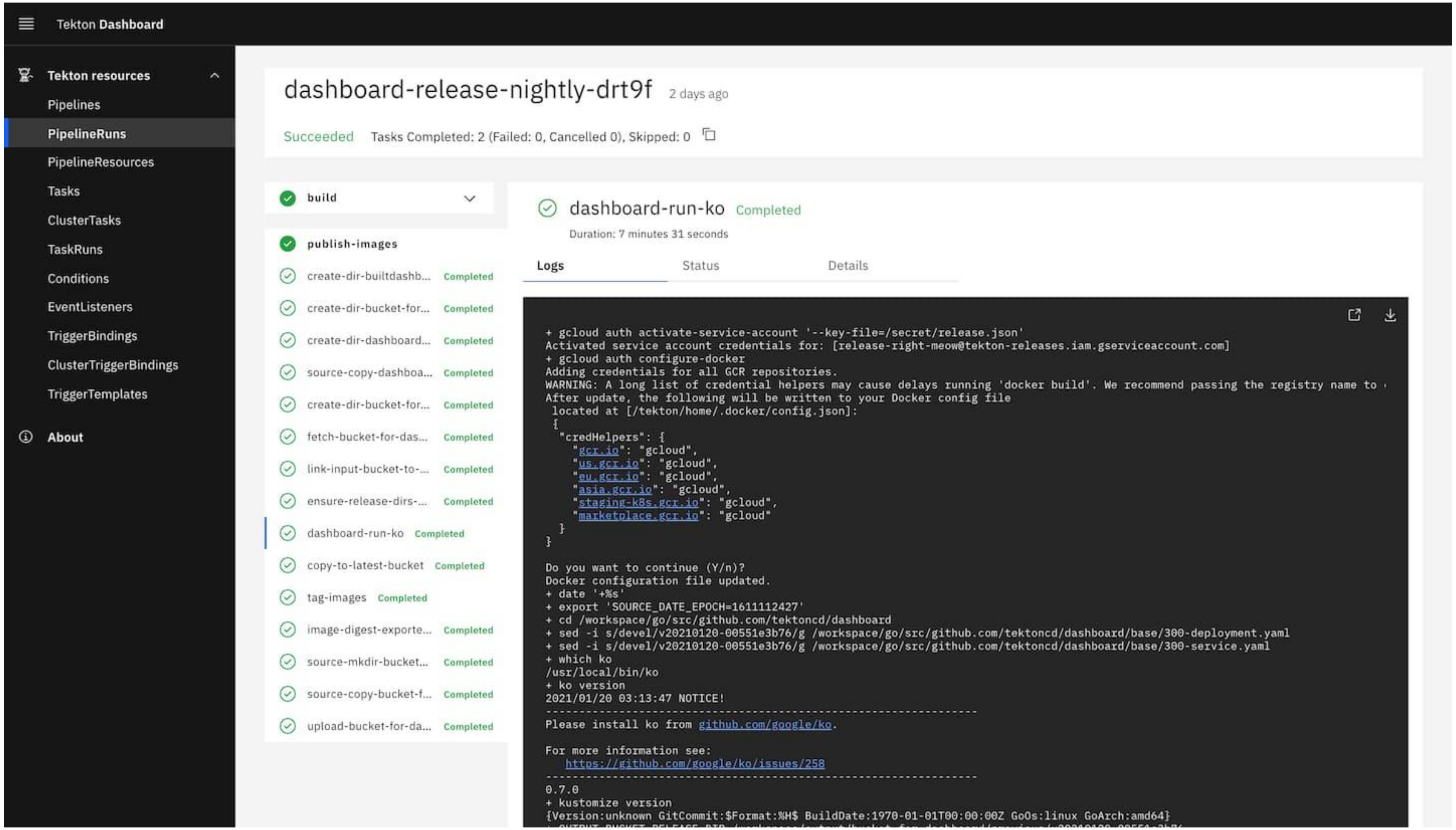


```yaml
apiVersion: triggers.tekton.dev/v1beta1
kind: TriggerTemplate
metadata:
  name: bitbucket-server-template
spec:
  params:
    - name: gitrevision
    - name: gitrepositoryurl
  resourcetemplates:
    - apiVersion: tekton.dev/v1beta1
      kind: TaskRun
      metadata:
        generateName: bitbucket-run-
      spec:
        taskSpec:
          steps:
            - image: ubuntu
              script: |
                #! /bin/bash
                echo "Revision is : $(tt.params.gitrevision). RepoURL is $(tt.params.gitrepositoryurl)"
```

https://github.com/tektoncd/triggers/blob/main/examples/v1beta1/bitbucket-server/triggertemplate.yaml

Tekton Dashboard

A (read-only) web-based UI for Tekton Pipelines and Tekton Triggers resources

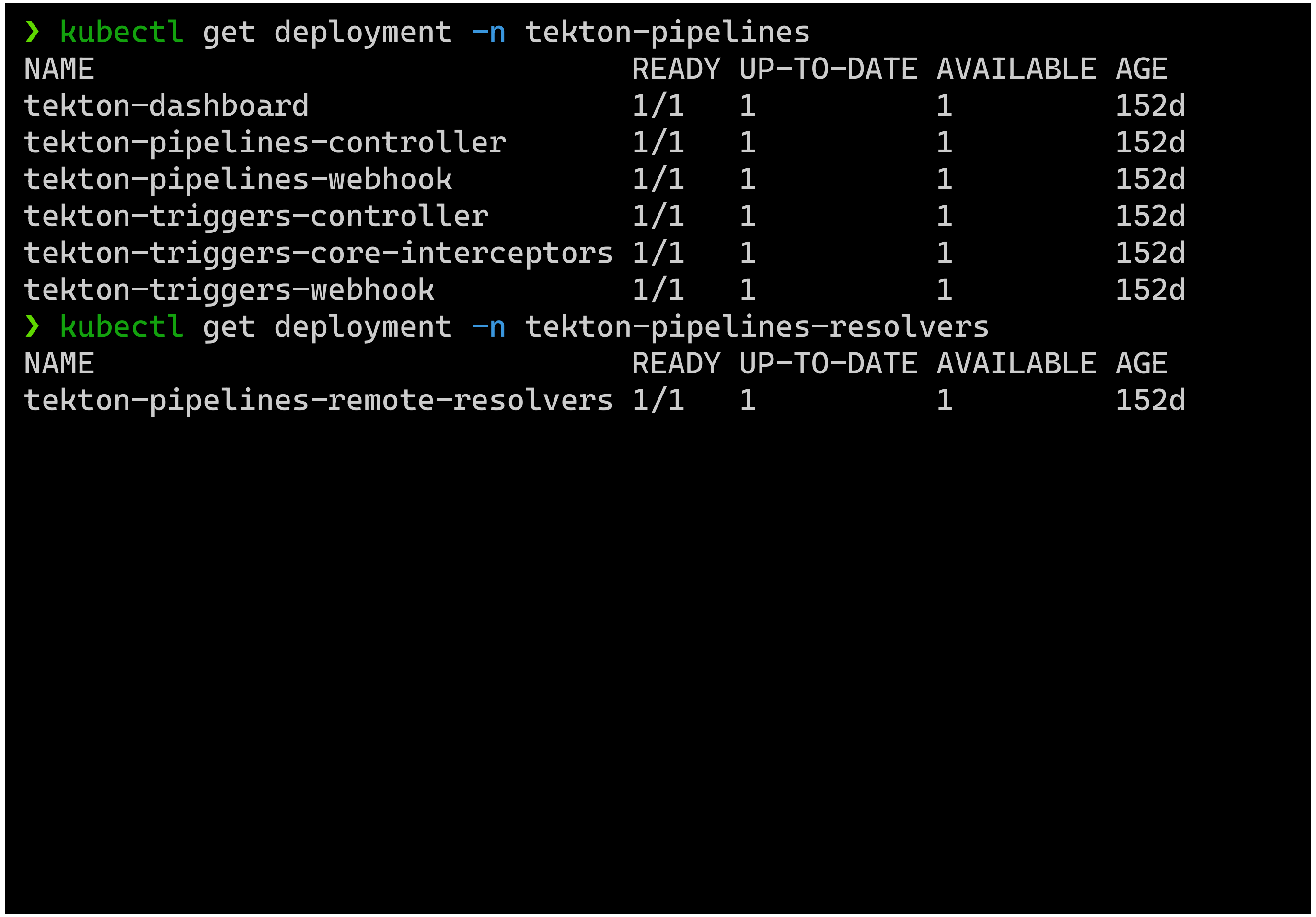

Tekton Dashboard
Tekton resources
Pipelines
PipelineRuns
PipelineResources
Tasks
ClusterTasks
TaskRuns
Conditions
EventListeners
TriggerBindings
ClusterTriggerBindings
TriggerTemplates
About
dashboard-release-nightly-drt9f
2 days ago
Succeeded
Tasks Completed: 2 (Failed: 0, Cancelled 0), Skipped: 0
build
publish-images
create-dir-builtdashb... Completed
create-dir-bucket-for... Completed
create-dir-dashboard... Completed
source-copy-dashboa... Completed
create-dir-bucket-for... Completed
fetch-bucket-for-das... Completed
link-input-bucket-to-... Completed
ensure-release-dirs-... Completed
dashboard-run-ko Completed
copy-to-latest-bucket Completed
tag-images Completed
image-digest-exporte... Completed
source-mkdir-bucket... Completed
source-copy-bucket-f... Completed
upload-bucket-for-da... Completed
dashboard-run-ko Completed
Duration: 7 minutes 31 seconds
Logs
Status
Details

```
+ gcloud auth activate-service-account '--key-file=/secret/release.json'
Activated service account credentials for: [release-right-meow@tekton-releases.iam.gserviceaccount.com]
+ gcloud auth configure-docker
Adding credentials for all GCR repositories.
WARNING: A long list of credential helpers may cause delays running 'docker build'. We recommend passing the registry name to
After update, the following will be written to your Docker config file
 located at [/tekton/home/.docker/config.json]:
 {
  "credHelpers": {
    "gcr.io": "gcloud",
    "us.gcr.io": "gcloud",
    "eu.gcr.io": "gcloud",
    "asia.gcr.io": "gcloud",
    "staging-k8s.gcr.io": "gcloud",
    "marketplace.gcr.io": "gcloud"
  }
}

Do you want to continue (Y/n)?
Docker configuration file updated.
+ date '+%s'
+ export 'SOURCE_DATE_EPOCH=1611112427'
+ cd /workspace/go/src/github.com/tektoncd/dashboard
+ sed -i s/devel/v20210120-00551e3b76/g /workspace/go/src/github.com/tektoncd/dashboard/base/300-deployment.yaml
+ sed -i s/devel/v20210120-00551e3b76/g /workspace/go/src/github.com/tektoncd/dashboard/base/300-service.yaml
+ which ko
/usr/local/bin/ko
+ ko version
2021/01/20 03:13:47 NOTICE!
-----------------------------------------------------------------
Please install ko from github.com/google/ko.

For more information see:
   https://github.com/google/ko/issues/258
-----------------------------------------------------------------
0.7.0
+ kustomize version
{Version:unknown GitCommit:$Format:%H$ BuildDate:1970-01-01T00:00:00Z GoOs:linux GoArch:amd64}
```

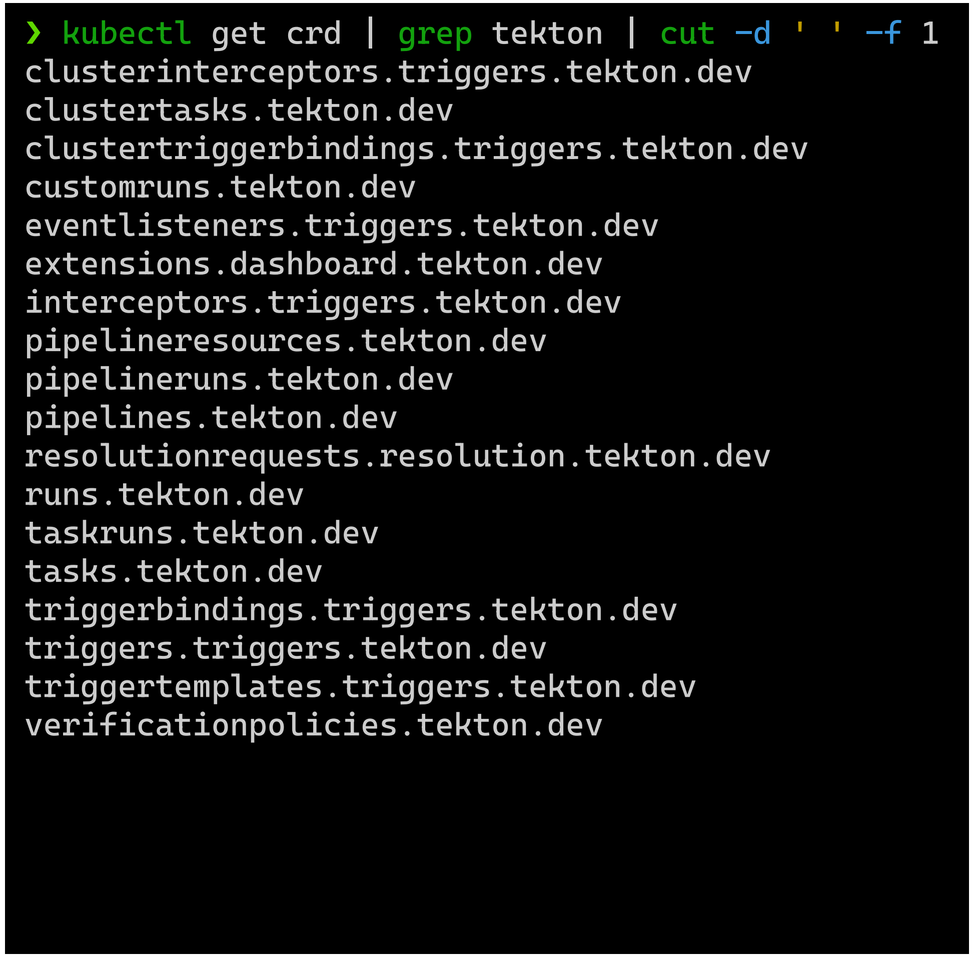
https://tekton.dev/docs/dashboard/dashboard-ui.jpg

Core Components

What you will have after install Tekton pipeline, trigger and trigger interceptor



```
❯ kubectl get deployment -n tekton-pipelines
NAME                              READY UP-TO-DATE AVAILABLE AGE
tekton-dashboard                  1/1   1          1         152d
tekton-pipelines-controller       1/1   1          1         152d
tekton-pipelines-webhook          1/1   1          1         152d
tekton-triggers-controller        1/1   1          1         152d
tekton-triggers-core-interceptors 1/1   1          1         152d
tekton-triggers-webhook           1/1   1          1         152d
❯ kubectl get deployment -n tekton-pipelines-resolvers
NAME                              READY UP-TO-DATE AVAILABLE AGE
tekton-pipelines-remote-resolvers 1/1   1          1         152d
```

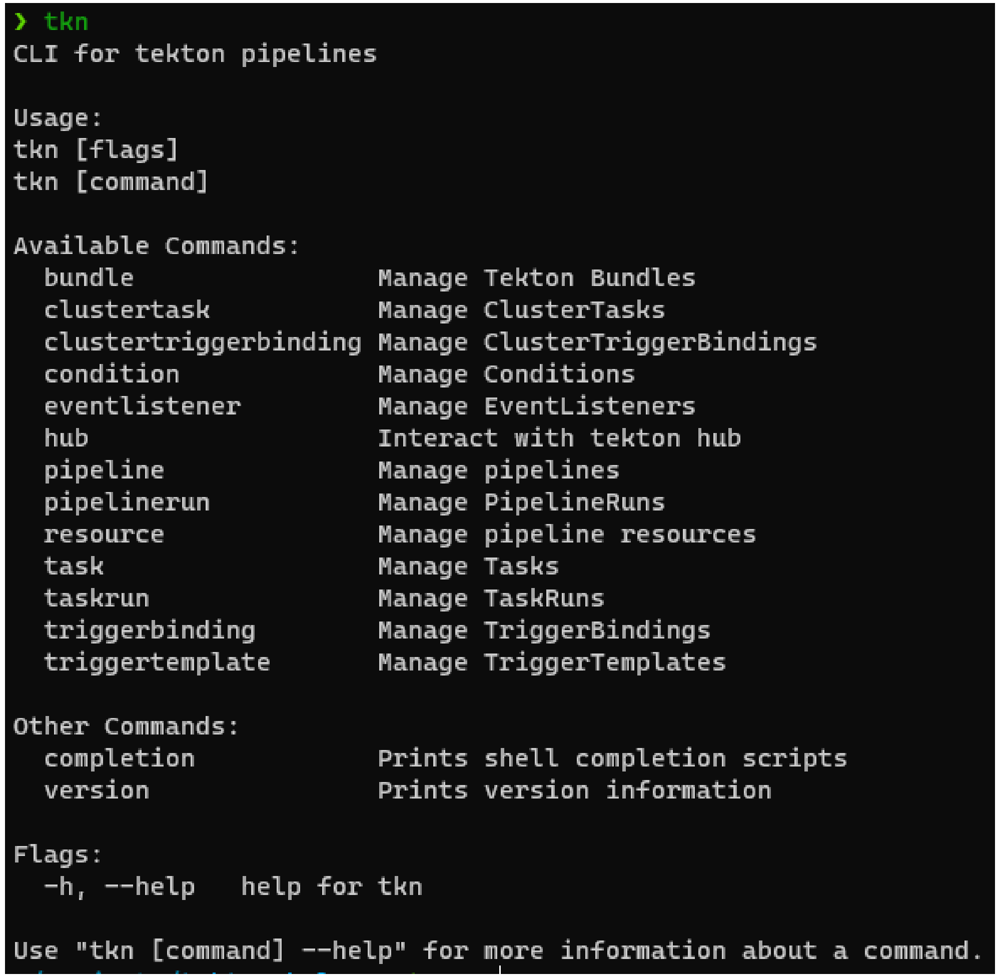


```
❯ kubectl get crd | grep tekton | cut -d ' ' -f 1
clusterinterceptors.triggers.tekton.dev
clustertasks.tekton.dev
clustertriggerbindings.triggers.tekton.dev
customruns.tekton.dev
eventlisteners.triggers.tekton.dev
extensions.dashboard.tekton.dev
interceptors.triggers.tekton.dev
pipelineresources.tekton.dev
pipelineruns.tekton.dev
pipelines.tekton.dev
resolutionrequests.resolution.tekton.dev
runs.tekton.dev
taskruns.tekton.dev
tasks.tekton.dev
triggerbindings.triggers.tekton.dev
triggers.triggers.tekton.dev
triggertemplates.triggers.tekton.dev
verificationpolicies.tekton.dev
```

https://tekton.dev/docs/installation/
https://tekton.dev/docs/dashboard/install/

Tekton Cli

A command line interface to interact with Tekton

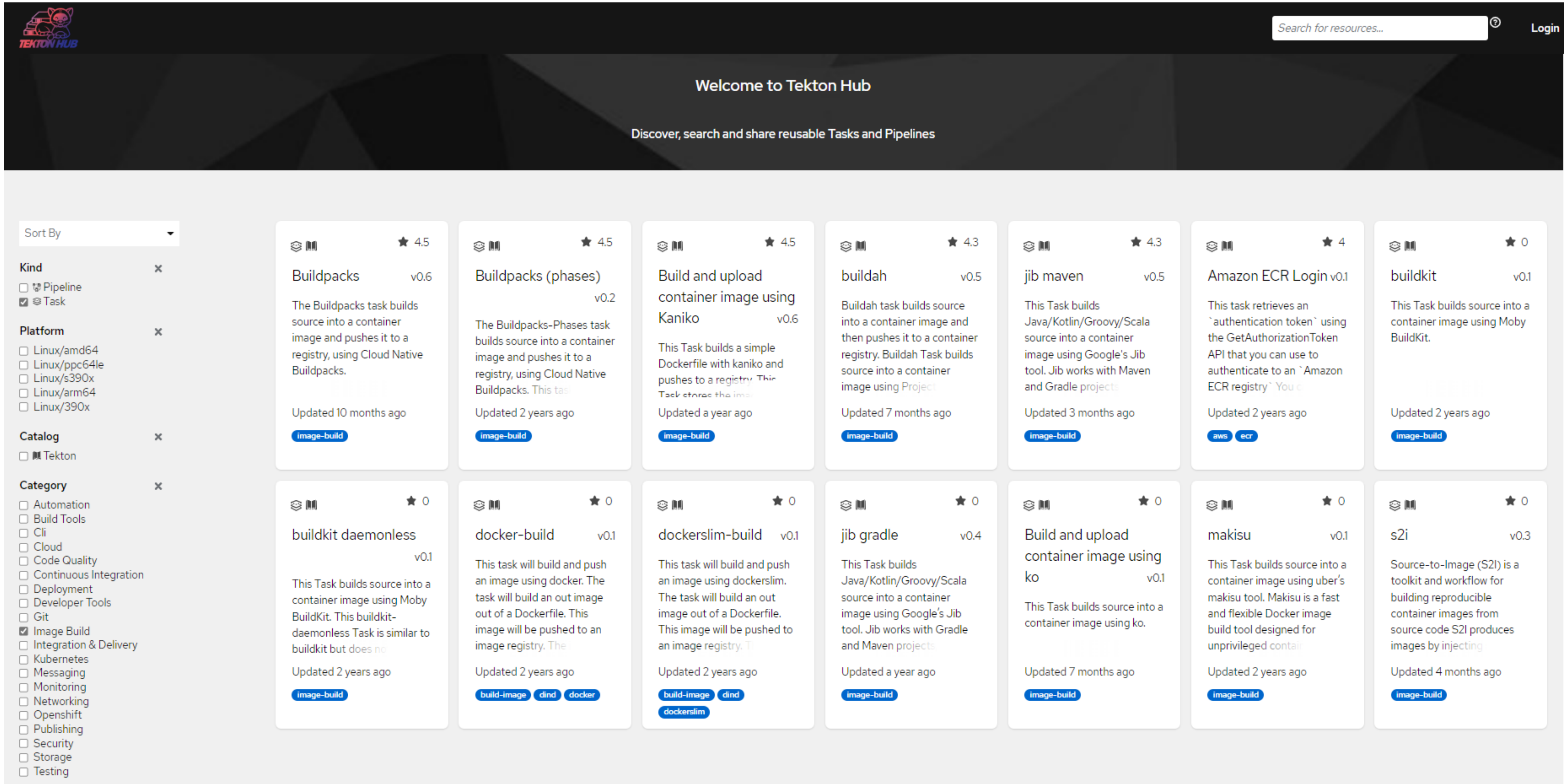


```
❯ tkn
CLI for tekton pipelines

Usage:
tkn [flags]
tkn [command]

Available Commands:
  bundle                Manage Tekton Bundles
  clustertask           Manage ClusterTasks
  clustertriggerbinding Manage ClusterTriggerBindings
  condition             Manage Conditions
  eventlistener         Manage EventListeners
  hub                   Interact with tekton hub
  pipeline              Manage pipelines
  pipelinerun           Manage PipelineRuns
  resource              Manage pipeline resources
  task                  Manage Tasks
  taskrun               Manage TaskRuns
  triggerbinding        Manage TriggerBindings
  triggertemplate       Manage TriggerTemplates

Other Commands:
  completion            Prints shell completion scripts
  version               Prints version information

Flags:
  -h, --help   help for tkn

Use "tkn [command] --help" for more information about a command.
```

https://tekton.dev/docs/cli/

Tekton Hub

A website to discover, search and share reusable Tasks and Pipelines



Welcome to Tekton Hub

Discover, search and share reusable Tasks and Pipelines

Sort By

Kind
- □ Pipeline
- ☑ Task

Platform
- □ Linux/amd64
- □ Linux/ppc64le
- □ Linux/s390x
- □ Linux/arm64
- □ Linux/390x

Catalog
- □ Tekton

Category
- □ Automation
- □ Build Tools
- □ Cli
- □ Cloud
- □ Code Quality
- □ Continuous Integration
- □ Deployment
- □ Developer Tools
- □ Git
- ☑ Image Build
- □ Integration & Delivery
- □ Kubernetes
- □ Messaging
- □ Monitoring
- □ Networking
- □ Openshift
- □ Publishing
- □ Security
- □ Storage
- □ Testing

★ 4.5 Buildpacks v0.6
The Buildpacks task builds source into a container image and pushes it to a registry, using Cloud Native Buildpacks.
Updated 10 months ago
image-build

★ 4.5 Buildpacks (phases) v0.2
The Buildpacks-Phases task builds source into a container image and pushes it to a registry, using Cloud Native Buildpacks. This tas
Updated 2 years ago
image-build

★ 4.5 Build and upload container image using Kaniko v0.6
This Task builds a simple Dockerfile with kaniko and pushes to a registry. This Task stores the ima
Updated a year ago
image-build

★ 4.3 buildah v0.5
Buildah task builds source into a container image and then pushes it to a container registry. Buildah Task builds source into a container image using Projec
Updated 7 months ago
image-build

★ 4.3 jib maven v0.5
This Task builds Java/Kotlin/Groovy/Scala source into a container image using Google's Jib tool. Jib works with Maven and Gradle projects
Updated 3 months ago
image-build

★ 4 Amazon ECR Login v0.1
This task retrieves an `authentication token` using the GetAuthorizationToken API that you can use to authenticate to an `Amazon ECR registry`. You c
Updated 2 years ago
aws ecr

★ 0 buildkit v0.1
This Task builds source into a container image using Moby BuildKit.
Updated 2 years ago
image-build

★ 0 buildkit daemonless v0.1
This Task builds source into a container image using Moby BuildKit. This buildkit-daemonless Task is similar to buildkit but does no
Updated 2 years ago
image-build

★ 0 docker-build v0.1
This task will build and push an image using docker. The task will build an out image out of a Dockerfile. This image will be pushed to an image registry. The
Updated 2 years ago
build-image dind docker

★ 0 dockerslim-build v0.1
This task will build and push an image using dockerslim. The task will build an out image out of a Dockerfile. This image will be pushed to an image registry. T
Updated 2 years ago
build-image dind dockerslim

★ 0 jib gradle v0.4
This Task builds Java/Kotlin/Groovy/Scala source into a container image using Google's Jib tool. Jib works with Gradle and Maven projects
Updated a year ago
image-build

★ 0 Build and upload container image using ko v0.1
This Task builds source into a container image using ko.
Updated 7 months ago
image-build

★ 0 makisu v0.1
This Task builds source into a container image using uber's makisu tool. Makisu is a fast and flexible Docker image build tool designed for unprivileged contai
Updated 2 years ago
image-build

★ 0 s2i v0.3
Source-to-Image (S2I) is a toolkit and workflow for building reproducible container images from source code S2I produces images by injecting
Updated 4 months ago
image-build

https://hub.tekton.dev/?category=Image+Build&kind=Task

Tips and Tricks

Helm is Your Best Friend on K8S

- A handy tool that help you to install/uninstall a set of objects
  - Tekton core components
  - Tasks, pipelines and Triggers in each namespace
- Helm values for different environment
- Helm installs resources in specific order, including namespace, CRD, Role, Binding and ServiceAccount, …
- helm-secrets for decrypt encrypted Helm values with sops and vals

powered by DALL·E 3

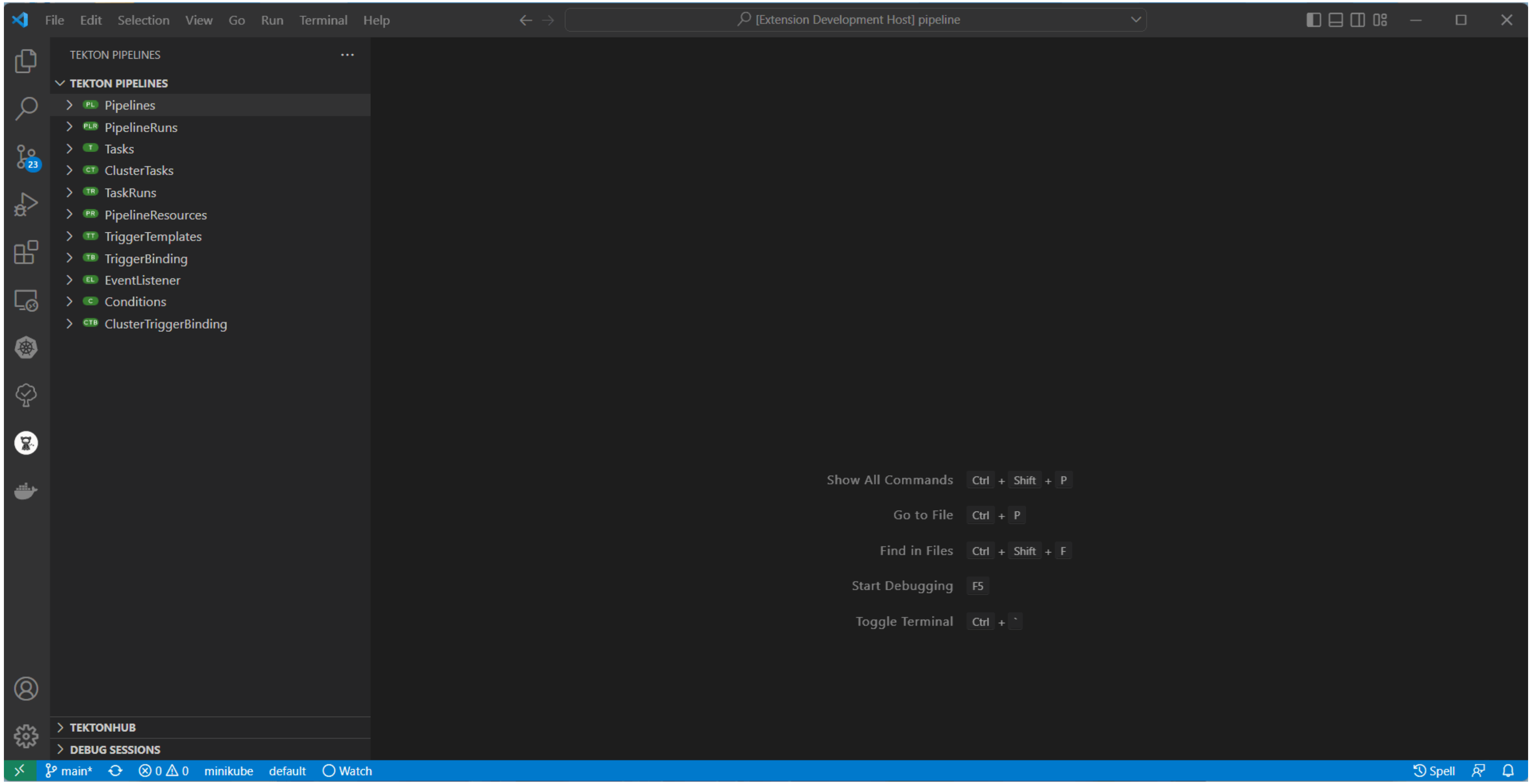
You Don’t Neet to Do Everything from Scratch

- Tekton Hub
- pipeline/examples at main · tektoncd/pipeline (github.com)
- triggers/examples at main · tektoncd/triggers (github.com)

powered by DALL·E 3

Use Visual Studio Code Plugin

UI with DAG visualization



Show All Commands Ctrl + Shift + P

Go to File Ctrl + P

Find in Files Ctrl + Shift + F

Start Debugging F5

Toggle Terminal Ctrl + `

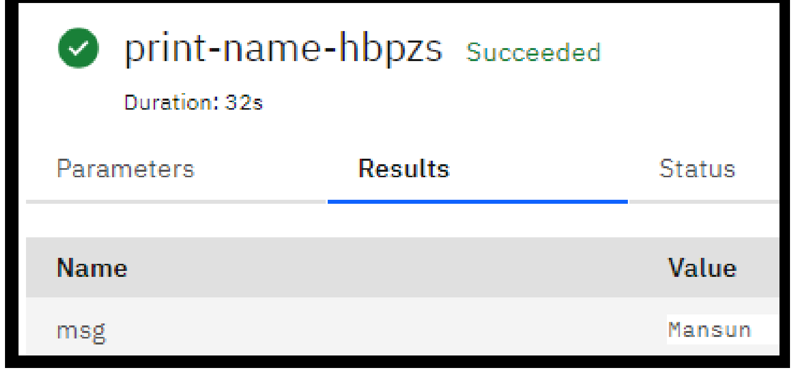
https://github.com/redhat-developer/vscode-tekton

Test Your Tekton Task

Move all params and paths of results as env vars for unit test

```yaml
# kubectl apply -f print-name.yaml
apiVersion: tekton.dev/v1
kind: Task
metadata:
  name: print-name
spec:
  params:
    - name: user
  results:
    - name: msg
  steps:
    - name: print-msg2
      image: docker.io/python:3.11.1-bullseye
      env:
        - name: USER
          value: $(params.user)
        - name: MSG_PATH
          value: $(results.msg.path)
      script: |
        #!/usr/bin/env python3
        import os
        with open(os.environ["MSG_PATH"] , "w", encoding="utf-8") as fout:
            fout.write(os.environ["USER"])
```

```yaml
# kubectl create -f print-name-tr.yaml
apiVersion: tekton.dev/v1
kind: TaskRun
metadata:
  generateName: print-name-
spec:
  serviceAccountName: default
  taskRef:
    kind: Task
    name: print
  params:
    - name: user
      value: Mansun
```



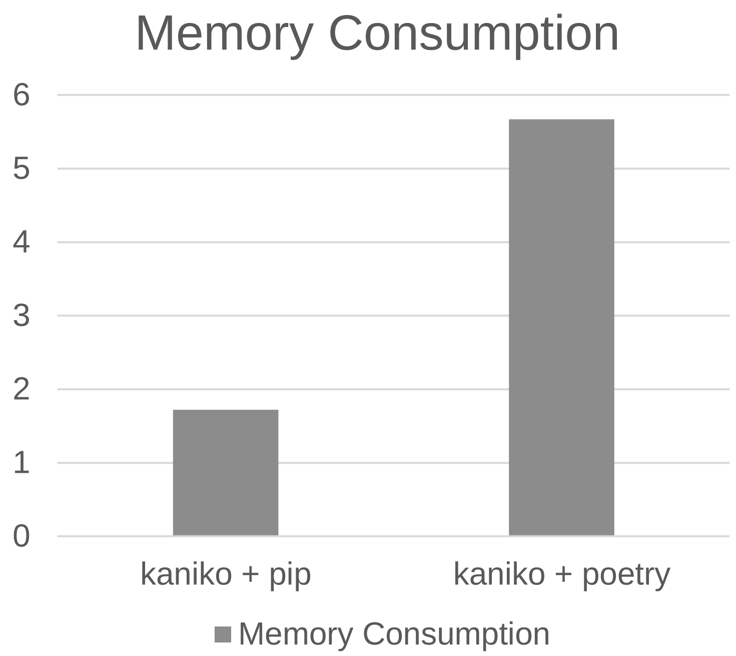
print-name-hbpzs Succeeded

Duration: 32s

Name	Value
msg	Mansun

Goodbye Docker, Hello Kaniko

- Familiar Dockerfile w/o Docker daemon
- Build layers and caches on registry
- Authentication
  - Workload identity with GKE service account
  - Cloud credential for GKE, ECR and AKS
  - Docker config.json
- Resource management
  - LimitRange
  - ResourceQuota
  - Resource request and limit in step
  - Task-level resource configuration(alpha)



https://raw.githubusercontent.com/GoogleContainerTools/kaniko/main/logo/Kaniko-Logo.png

RBAC

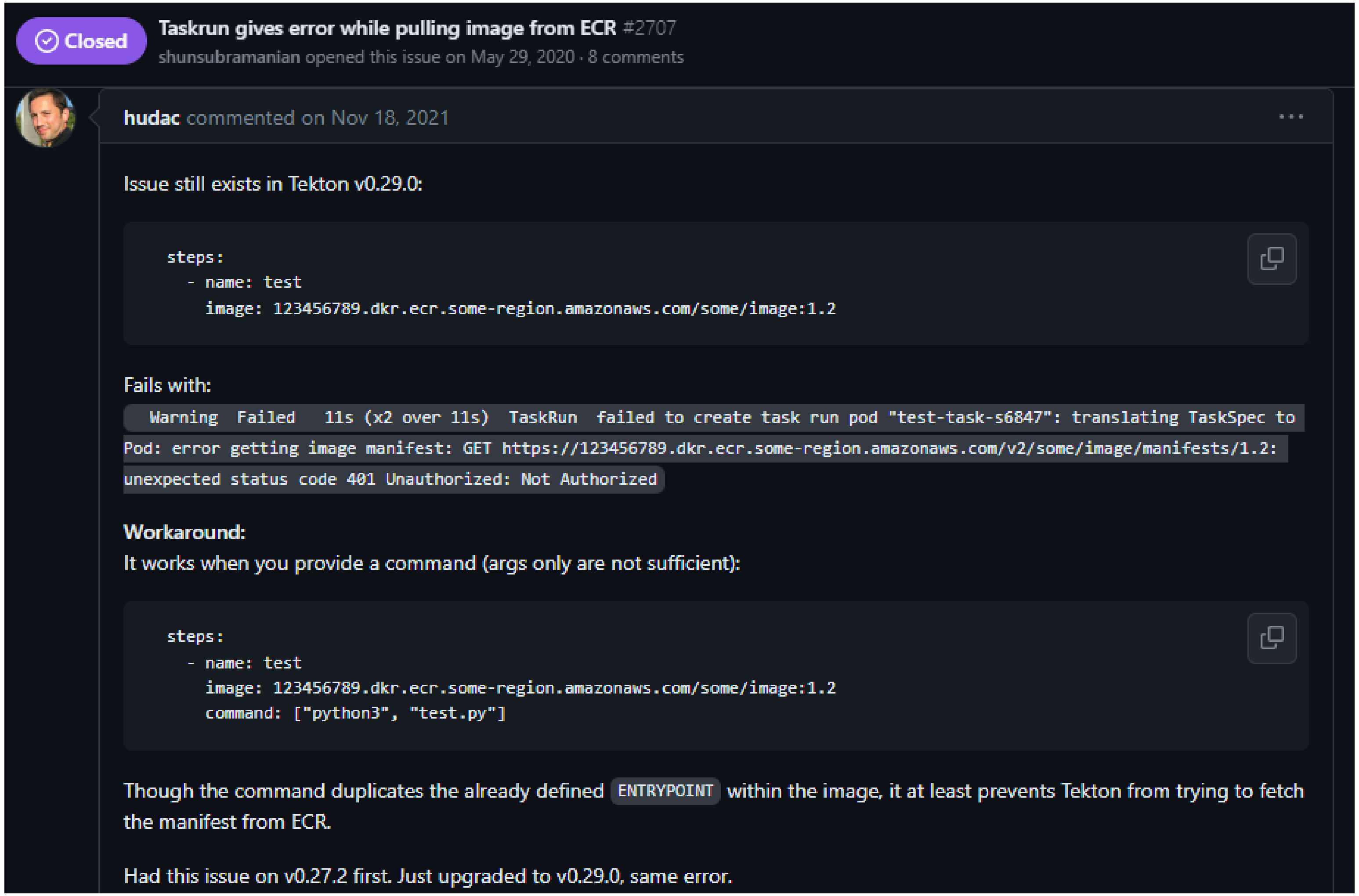
Set appropriate permissions and binding for your cluster. Be ware of aggregated ClusterRole.

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: tekton-triggers-eventlistener-clusterroles
  labels:
    app.kubernetes.io/instance: default
    app.kubernetes.io/part-of: tekton-triggers
rules:
  - apiGroups: ["triggers.tekton.dev"]
    resources: ["clustertriggerbindings", "clusterinterceptors"]
    verbs: ["get", "list", "watch"]
  # - apiGroups: [""]
  #   resources: ["secrets"]
  #   verbs: ["get", "list", "watch"]
```

https://github.com/tektoncd/triggers/blob/v0.25.0/config/200-clusterrole.yaml#L110-L123
https://github.com/tektoncd/triggers/blob/v0.25.0/config/clusterrole-aggregate-edit.yaml#L28-L29

Caveat of Tekton Task

- Need to lookup the entrypoint if the step doesn’t specify command
  - Might need credentials to read container image config
- Solutions
  - Provide command
  - Host all tasks on our own
  - Use Helm to manages and deploy tasks and pipelines



Taskrun gives error while pulling image from ECR #2707

shunsubramanian opened this issue on May 29, 2020 · 8 comments

hudac commented on Nov 18, 2021

Issue still exists in Tekton v0.29.0:

```
steps:
  - name: test
    image: 123456789.dkr.ecr.some-region.amazonaws.com/some/image:1.2
```

Fails with:

```
  Warning  Failed   11s (x2 over 11s)  TaskRun  failed to create task run pod "test-task-s6847": translating TaskSpec to
Pod: error getting image manifest: GET https://123456789.dkr.ecr.some-region.amazonaws.com/v2/some/image/manifests/1.2:
unexpected status code 401 Unauthorized: Not Authorized
```

Workaround:
It works when you provide a command (args only are not sufficient):

```
steps:
  - name: test
    image: 123456789.dkr.ecr.some-region.amazonaws.com/some/image:1.2
    command: ["python3", "test.py"]
```

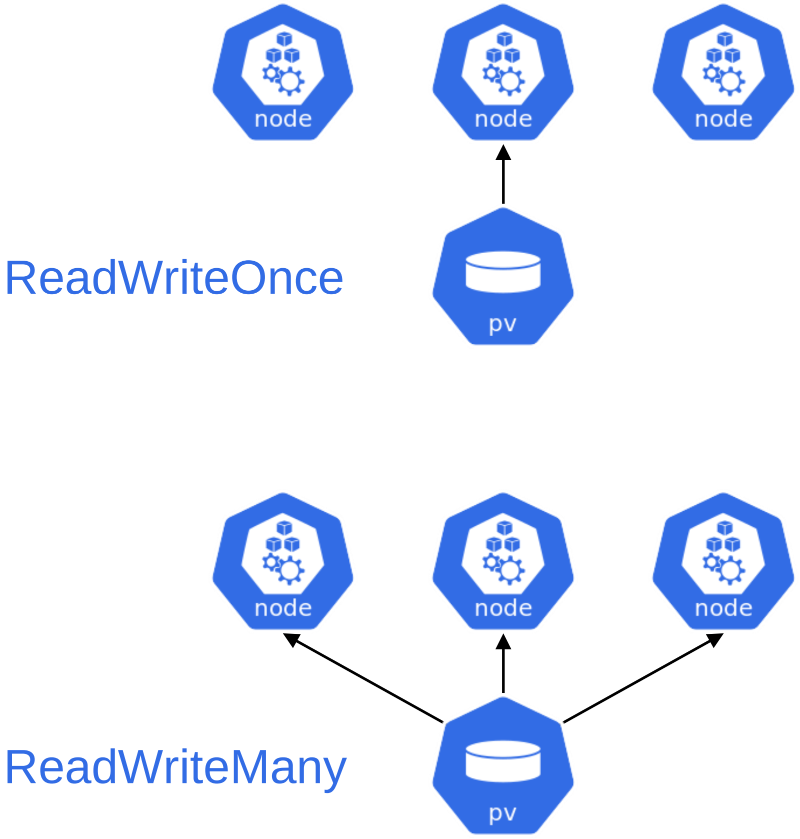
Though the command duplicates the already defined `ENTRYPOINT` within the image, it at least prevents Tekton from trying to fetch the manifest from ECR.

Had this issue on v0.27.2 first. Just upgraded to v0.29.0, same error.

https://www.youtube.com/watch?v=iz9_omZ0ctk&t=874s
https://github.com/tektoncd/pipeline/issues/2707#issuecomment-972417727

Affinity and PVC Workspace

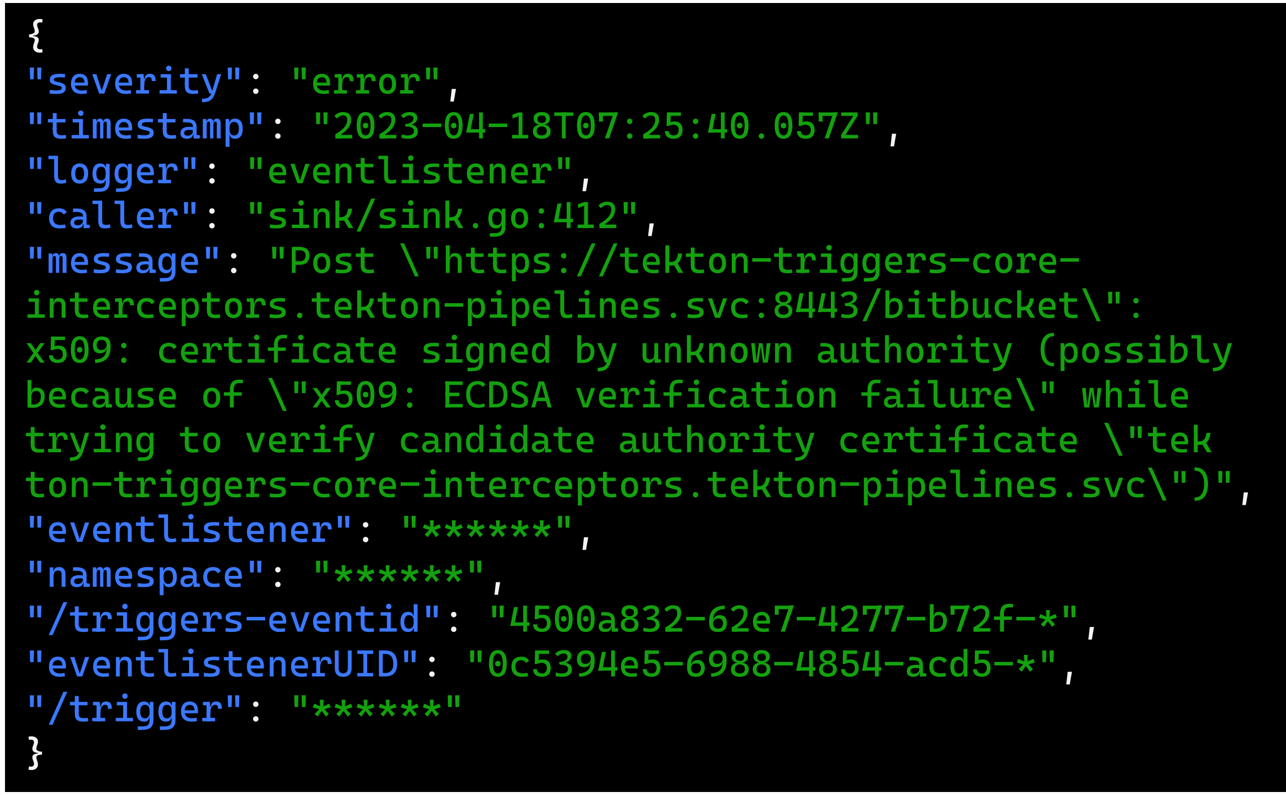
- Affinity assistant is enabled by default to make it possible to run parallel with ReadWriteOnce persistent volume
  - Inter-pod affinity
    - requiredDuringSchedulingIgnoredDuringExecution
- Pipeline stop working when a node is full of pods
- Solutions
  - Use ReadWriteMany persistent volume
  - Disable affinity assistant and use inter-pod affinity in pipelineRun
    - preferredDuringSchedulingIgnoredDuringExecution



https://github.com/tektoncd/pipeline/pull/2630
https://github.com/kubernetes/community/tree/master/icons

x509 Certificate Error of Cluster Interceptor

- Tekton trigger enabled HTTPS since v.0.20.0
- While installing Triggers Interceptors with empty secret, it generate cert and key internally
- We found random x509 cert error after GKE cluster rolling upgrade
- Solutions:
  - Use fixed cert and key to install it



```
{
"severity": "error",
"timestamp": "2023-04-18T07:25:40.057Z",
"logger": "eventlistener",
"caller": "sink/sink.go:412",
"message": "Post \"https://tekton-triggers-core-
interceptors.tekton-pipelines.svc:8443/bitbucket\":
x509: certificate signed by unknown authority (possibly
because of \"x509: ECDSA verification failure\" while
trying to verify candidate authority certificate \"tek
ton-triggers-core-interceptors.tekton-pipelines.svc\")",
"eventlistener": "******",
"namespace": "******",
"/triggers-eventid": "4500a832-62e7-4277-b72f-*",
"eventlistenerUID": "0c5394e5-6988-4854-acd5-*",
"/trigger": "******"
}
```

https://github.com/tektoncd/community/blob/main/teps/0102-https-connection-to-triggers-interceptor.md

Key Takeaways

Key Takeaways

- Focus on business value, not tool itself
- Existed tool of whole organization first
- Get buy-in from your manager
- Have a PoC
- Build your credits
- Find allies
- Marketing for your ideas
- Be persistent

https://tekton.dev/partner-logos/tekton-friends.png

Reference

- Cloud native
  - What is Cloud Native? - Cloud Native Applications Explained - AWS (amazon.com)
- CI/CD
  - Continuous integration vs. delivery vs. deployment (atlassian.com)
- Tekton
  - Getting Started | Tekton
  - Next Generation CI/CD with GKE and Tekton (Cloud Next '19) - YouTube
  - Tekton Graduation | Tekton
  - [question] How does tekton control the order of the steps in task · Issue #3782
- Helm
  - Helm | Using Helm
  - jkroepke/helm-secrets: A helm plugin that help manage secrets with Git workflow
- Mindset
  - Five tips for how to bring a new DevOps tool to your team | CircleCI
  - Software Architect Roadmap