



SOSS Community Day

EUROPE



SOSS Community Day
EUROPE

Let devs be devs without sacrificing security

Andrew McNamara; Red Hat

What does it mean to be a developer?

Build off of open source software

Explore new problem spaces and solutions

Use tooling that is supportive not disruptive

Devs want to easily build artifacts

[festoji / .github / workflows / package.yaml](#) ↗

arewm update slsa provenance generator ✓

Code Blame 90 lines (75 loc) · 2.67 KB

```
1  ---
2  name: Package
3
4  on:
5    push:
6      workflow_dispatch:
7
8  env:
9    IMAGE_REGISTRY: quay.io
10   IMAGE_REPO: arewm/festoji
11   IMAGE_TAGS: latest
12
13  jobs:
14    build:
```



Devs want to troubleshoot builds

[festoji / .github / workflows / package.yaml](#) ↗

arewm update slsa provenance generator ✓

Code Blame 90 lines (75 loc) · 2.67 KB

```
1 ---  
2   name: Package  
3  
4   on:  
5     push:  
6       workflow_dispatch:  
7  
8   env:  
9     IMAGE_REGISTRY: quay.io  
10    IMAGE_REPO: arewm/festoji  
11    IMAGE_TAGS: latest  
12  
13  jobs:  
14    build:
```



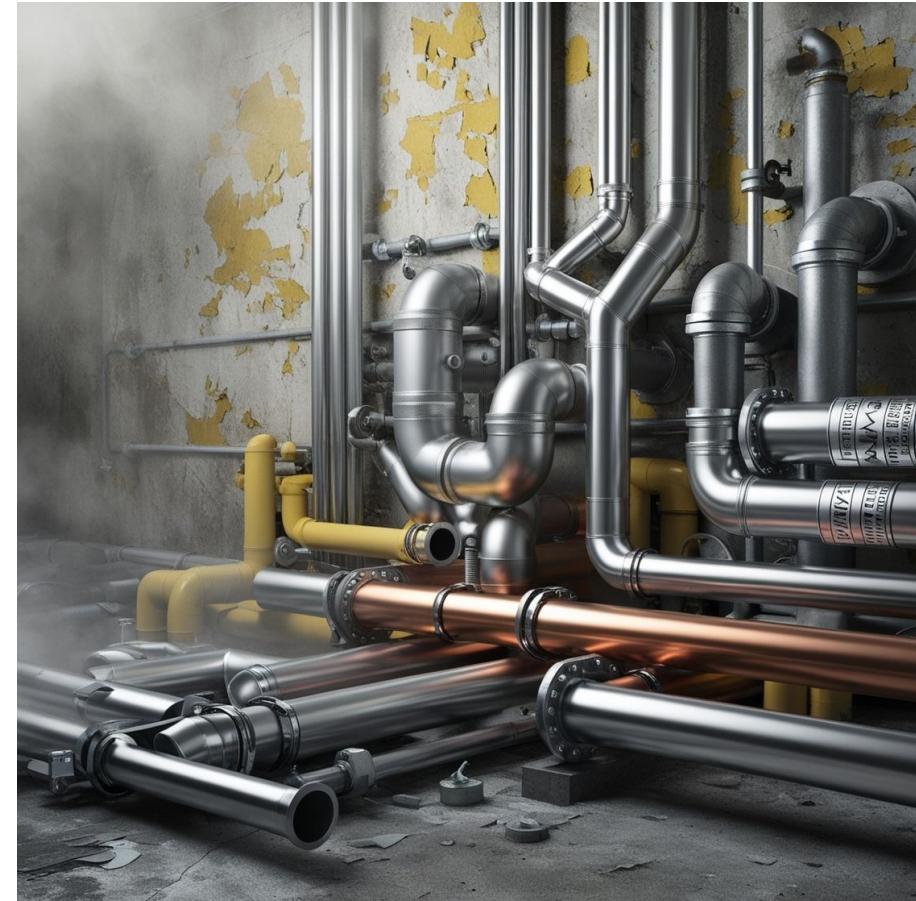
Devs want to explore new tech

[festoji / .github / workflows / package.yaml](#) 

 arewm update slsa provenance generator ✓

Code Blame 90 lines (75 loc) · 2.67 KB

```
1  ---
2  name: Package
3
4  on:
5    push:
6      workflow_dispatch:
7
8  env:
9    IMAGE_REGISTRY: quay.io
10   IMAGE_REPO: arewm/festoji
11   IMAGE_TAGS: latest
12
13  jobs:
14    build:
```



Devs don't need to be this unhappy

SLSA Build L3:
Harden the build platform

Generate provenance

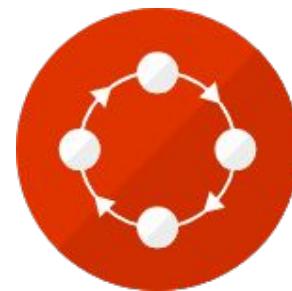


Devs don't need to be this unhappy

Focus on hardening the build platform



Focus on accurate (detailed) provenance



Provide templates for builds and tests

Devs don't need to be this unhappy

Flexibility vs. risk

Sliding scale of risk



enterprise
contract

Devs can easily build artifacts

The screenshot shows a GitHub interface with the following navigation tabs:

- Conversation 0
- Commits 1
- Checks 6
- Files changed 2 (highlighted)

Below the tabs, there are filters: "Changes from all commits" (dropdown), "File filter" (dropdown), "Conversations" (dropdown), and a settings gear icon.

A search bar labeled "Filter changed files" is present.

The main content area displays a file change summary for ".tekton/festoji-pull-request.yaml":

- 452 changes (represented by green squares)
- 1,452 lines added (green background)
- 3 lines added (blue background)

The added lines are:

```
1 + apiVersion: tekton.dev/v1
2 + kind: PipelineRun
3 + metadata:
```

Devs can easily build artifacts

Results

Component ▾ Status ▾ Filter by rule...

Results summary

! Failed 14 ! Warning 3 ✓ Success 94

Rules	Status	Message	Component
> Build task called with hermetic param set	! Failed	Build task was not invoked with the hermetic parameter set	festoji
> Required labels	! Failed	The required "com.redhat.component" label is missing. La...	festoji
> Required labels	! Failed	The required "description" label is missing. Label descripti...	festoji
> Exists	! Failed	No source image references found	festoji
> All required tasks were included in the pipeline	! Failed	One of "source-build", "source-build-oci-ta" tasks is missi...	festoji
> No tests erred	! Failed	The Task "ecosystem-cert-preflight-checks" from the buil...	festoji
> No tests were skipped	! Failed	The Task "sast-snyk-check-oci-ta" from the build Pipeline...	festoji
> Optional labels	! Warning	The optional "maintainer" label is missing. Label descripti...	festoji

Devs can troubleshoot builds

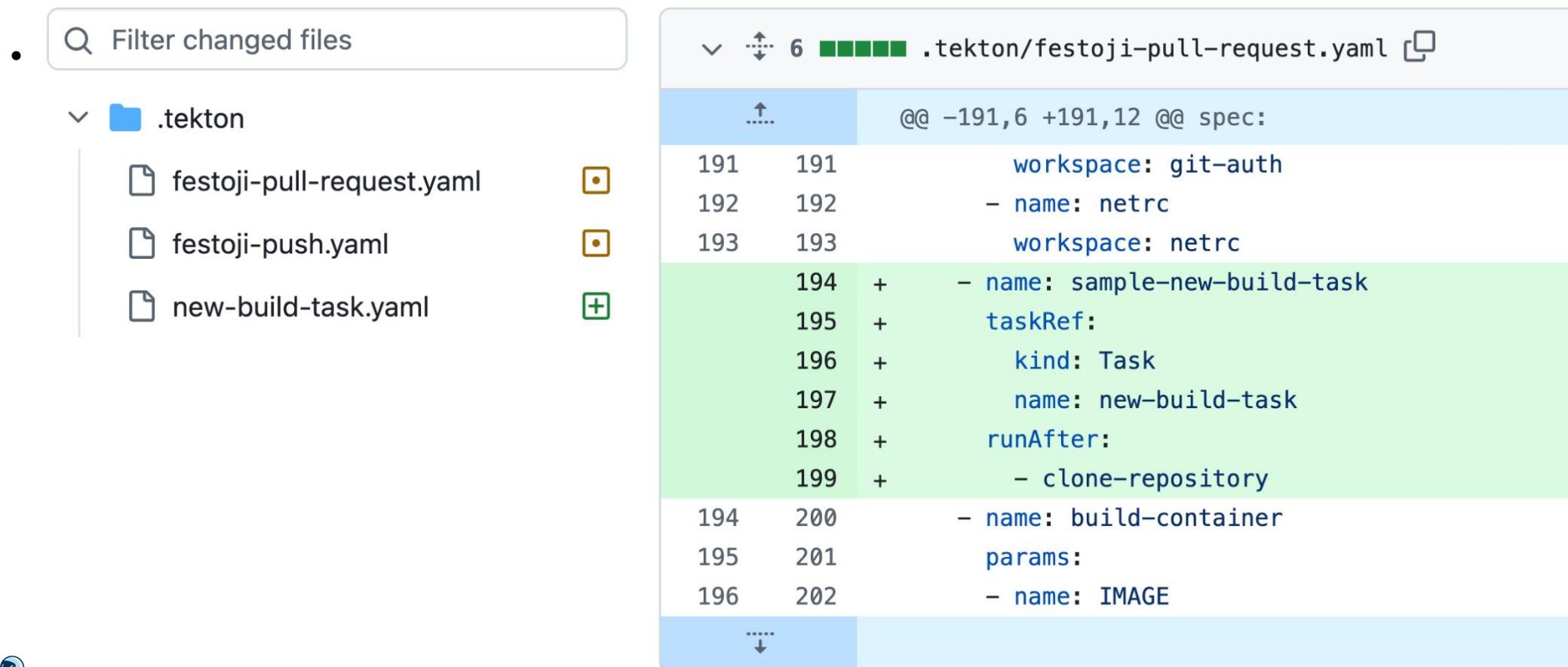
```
taskRef:  
  params:  
    - name: name  
      value: buildah-oci-ta  
    - name: bundle  
      value: quay.io/konflux-ci/tekton-catalog/task-buildah-oci-ta:0.2  
    - name: kind  
      value: task  
resolver: bundles
```

Devs can troubleshoot builds

```
$ tkn bundle list -o json quay.io/konflux-ci/tekton-catalog/task-buildah-oci-ta
:0.2 task buildah-oci-ta | jq
{
  "kind": "Task",
  "apiVersion": "tekton.dev/v1",
  "metadata": {
    "name": "buildah-oci-ta",
    "creationTimestamp": null,
    "labels": {
      "app.kubernetes.io/version": "0.2",
      "build.appstudio.redhat.com/build_type": "docker"
    },
    "annotations": {
      "tekton.dev/pipelines.minVersion": "0.12.1",
      "tekton.dev/tags": "image-build, konflux"
    }
  },
  "spec": [
    ...
  ]
}
```



Devs can explore new tech



The screenshot shows a diff tool interface comparing two versions of a YAML file. The left pane displays the file structure:

- Filter changed files
- .tekton folder
 - festoji-pull-request.yaml
 - festoji-push.yaml
 - new-build-task.yaml

The right pane shows the diff output for the .tekton/festoji-pull-request.yaml file. The changes are color-coded: red for deleted lines and green for added lines. A specific section of the file is highlighted in green, indicating it has been modified.

```
diff --git a/.tekton/festoji-pull-request.yaml b/.tekton/festoji-pull-request.yaml
--- a/.tekton/festoji-pull-request.yaml
+++ b/.tekton/festoji-pull-request.yaml
@@ -191,6 +191,12 @@ spec:
 191  191      workspace: git-auth
 192  192      - name: netrc
 193  193      workspace: netrc
+194  +      - name: sample-new-build-task
+195  +      taskRef:
+196  +      kind: Task
+197  +      name: new-build-task
+198  +      runAfter:
+199  +      - clone-repository
 194  200      - name: build-container
 195  201          params:
 196  202          - name: IMAGE
```

Devs don't need to be this unhappy



Thank you!

