Secure Supply Chain at Home

TektonCD

Andrew Thorp

Red Hat

Nov 09, 2026

KubeCon CloudNativeCon
North America 2026

Goals

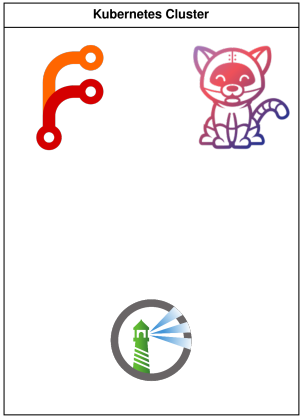
What do we want

- Compile and build container images
- Automated, portable builds
- Secure, self-hosted build runners
- Verifiable, attested builds
- Don't get hacked

Setup

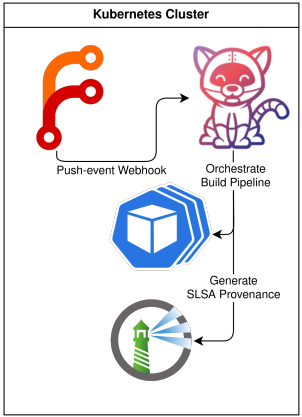
Environment

- **git Forge**
  - Forgejo, GitLab, etc
- **Platform**
  - TektonCD running on Kubernetes
- **Container Registry**
  - Harbor, Zot, etc



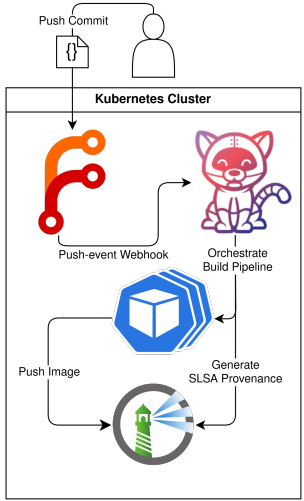
TektonCD

- **Tekton Pipelines**
  - Orchestration engine
- **Tekton Pipelines as Code**
  - git forge↔Tekton bridge
- **Tekton Chains**
  - Generate attestations, signs images



Workflow Overview

1. Push commit
2. Forgejo sends webhook to Pipelines as Code
3. Tekton executes PipelineRun in cluster
4. PipelineRun clones, vendors, builds, and pushes the build
5. Tekton Chains attests and signs the image

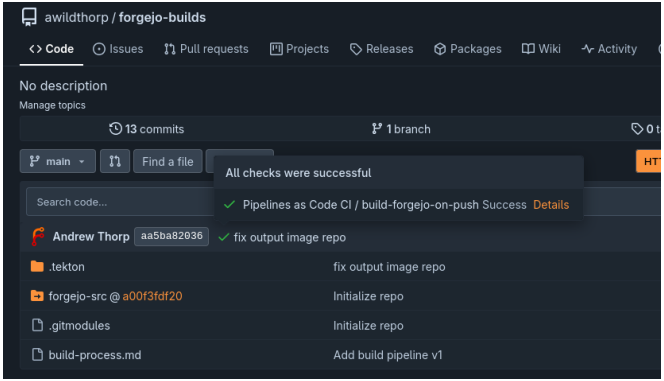


Buld Pipeline

```yaml
apiVersion: tekton.dev/v1
kind: PipelineRun
spec:
  pipelineSpec:
    tasks:  # <- Each Task runs in separate Pod
      - name: clone-repo
        ...
      - name: prefetch-dependencies
        ...
      - name: build
        taskSpec:
          metadata:
            annotations:
              experimental.tekton.dev/execution-mode: hermetic
        ...
      - name: push-image
        ...
      - name: bundle-sbom-etc
        ...
```

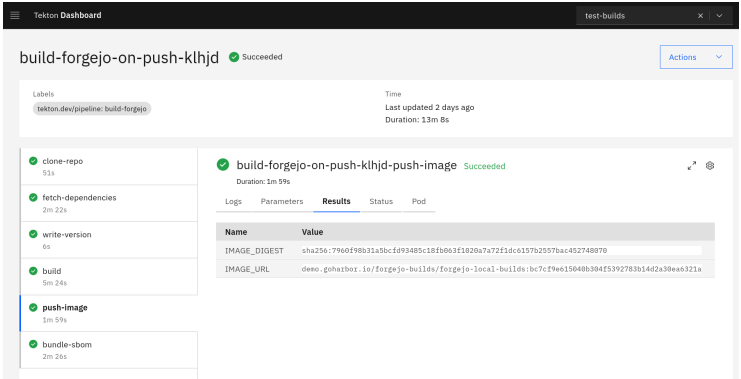
Outcome

Git Commit Status



git Commit status post-build

PipelineRun



Build PipelineRun in the Tekton Dashboard

Provenance Generated

Tekton Chains generated attestation, SLSA provenance

```
~/c/forgejo-builds (main|✓) $ cosign tree demo.goharbor.io/forgejo-builds/forgejo-local-builds:bc7cf9e615040b304f5392783b14d2a30ea6321a
📦 Supply Chain Security Related artifacts for an image: demo.goharbor.io/forgejo-builds/forgejo-local-builds:bc7cf9e615040b304f5392783b14d2a30ea6
321a
└── 💾 Attestations for an image tag: demo.goharbor.io/forgejo-builds/forgejo-local-builds:sha256-7960f98b31a5bcfd93485c18fb063f1020a7a72f1dc6157b
2557bac452748070.att
    ├── 🍒 sha256:da14bebf901321f46fd3fe3bfc605415ed335321e65ec779b725a0d5f75d0249
    └── 🍒 sha256:54a14096e44152c8d8bc8ccd77ce91c155b41ee5012c9408da3a87cd16dda525
└── 🔐 Signatures for an image tag: demo.goharbor.io/forgejo-builds/forgejo-local-builds:sha256-7960f98b31a5bcfd93485c18fb063f1020a7a72f1dc6157b25
57bac452748070.sig
    └── 🍒 sha256:3a61b87d5abf60e2c22483f8dcd205afd2a5888565b8c433120c27580fc69e75
~/c/forgejo-builds (main|✓) $ cosign verify-attestation --key cosign.pub  demo.goharbor.io/forgejo-builds/forgejo-local-builds:bc7cf9e615040b304f5
392783b14d2a30ea6321a --type=slsaprovenance

Verification for demo.goharbor.io/forgejo-builds/forgejo-local-builds:bc7cf9e615040b304f5392783b14d2a30ea6321a --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - Existence of the claims in the transparency log was verified offline
  - The signatures were verified against the specified public key
{"payloadType":"application/vnd.in-toto+json","payload":"eyJfdHlwZSI6Imh0dHBzOi8vaW4tdG90by5pby9TdGF0ZW1lbnQvdjAuMSIsICJzdWJqZWN0IjpbeyJuYW1lIjoiZ
GVtby5nb2hhcmJvci5pby9mb3JnZWpvLWJ1aWxkcy9mb3JnZWpvLWxvY2FsLWJ1aWxkcyIsICJkaWdlc3QiOnsic2hhMjU2IjoiNzk2MGY5OGIzMWE1YmNmZDkzNDg1YzE4ZmIwNjNmMTAyMGE
3YTcyZjFkYzYxNTdiMjU1N2JhYzQ1Mjc0ODA3MCJ9fV0sICJwcmVkaWNhdGVUeXBlIjoiaHR0cHM6Ly9zbHNhLmRldi9wcm92ZW5hbmNlLzAicHJlZGljYXRlIjp7ImJ1aWxkQ29uZ
...
```

Cosign verification

Conclusion

- Automated build on `git push` to Forgejo, GitLab, GitHub, etc
- Build executed in controlled, **network-isolated** environment
- **SLSA Provenance automatically generated** by Tetkon Chains

Come See Us At The Project Pavilion

Presentation Source



TektonCD

Supply Chain Security at Home: From Source to Service Without the Hassle

Feedback