

ghasum: Integrity for GitHub Actions

Eric Cornelissen (ericco@kth.se)



This work is licensed under a
Creative Commons Attribution 4.0 International License (CC BY 4.0)

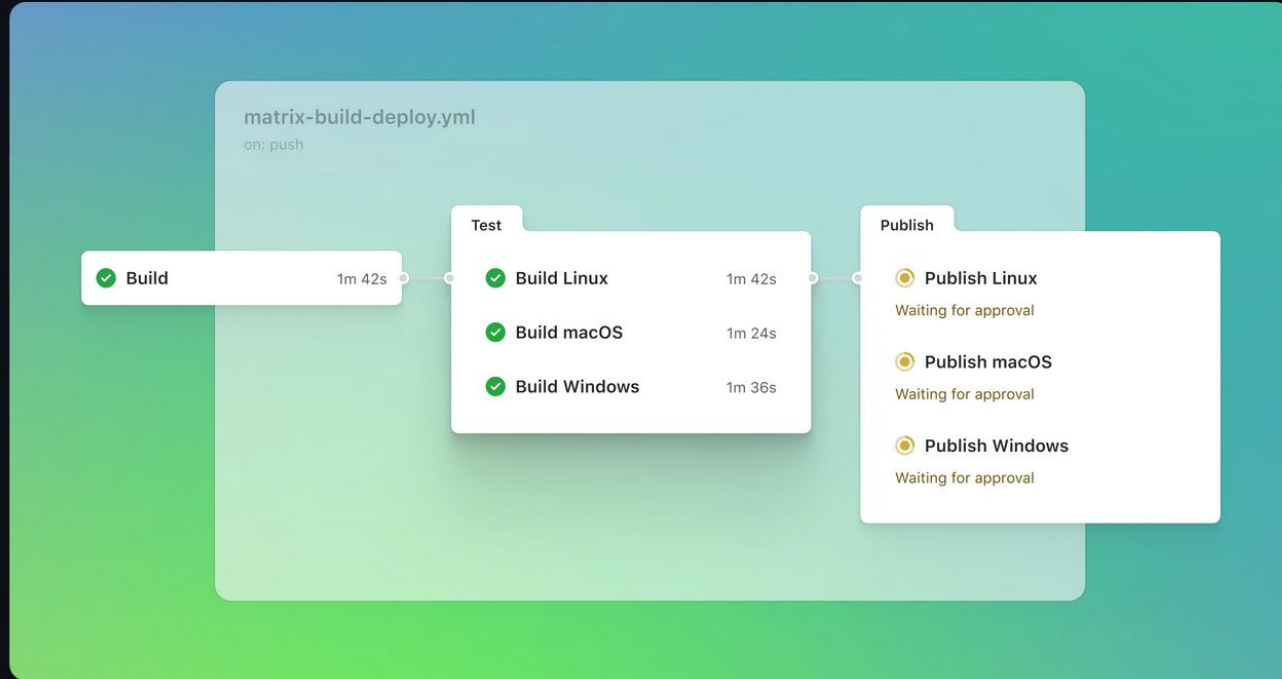
Overview

- Background
- Tool
- Demo
- Roadmap
- Takeaways

Background

- GitHub Actions
 - Continuous Integration & Deployment system

Get started



source: <https://github.com/features/actions>

Background

- GitHub Actions
 - Continuous Integration & Deployment system
 - Reusable components called "Actions"

```
14     steps:  
15     - name: Checkout repository  
16       uses: actions/checkout@v4.2.0
```

Background

- GitHub Actions
 - Continuous Integration & Deployment system
 - Reusable components called "Actions"

```
14     steps:  
15     - name: Checkout repository  
16       uses: actions/checkout@v4.2.0
```

Background

- GitHub Actions
 - Continuous Integration & Deployment system
 - Reusable components called "Actions"
 - Versioned using git refs

16

```
uses: actions/checkout@v4.2.0
```



git tag

Background

- GitHub Actions
 - Continuous Integration & Deployment system
 - Reusable components called "Actions"
 - Versioned using git refs

16

```
uses: actions/checkout@3f3598b
```

git tag

commit sha

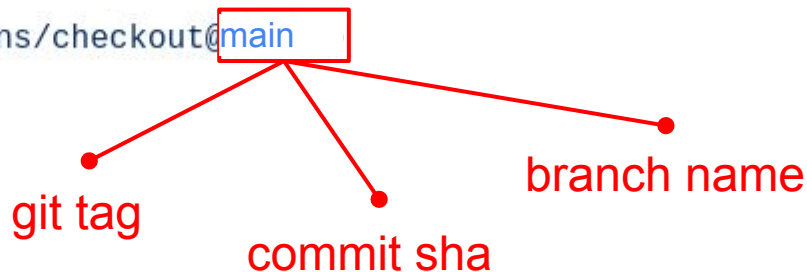


Background

- GitHub Actions
 - Continuous Integration & Deployment system
 - Reusable components called "Actions"
 - Versioned using git refs

16

```
uses: actions/checkout@main
```



Background

- GitHub Actions
 - Continuous Integration system
 - Reusable components called "Actions"
 - Versioned using git refs (*branch name, git tag, commit sha*)
 - Fetched at runtime

```
16      uses: actions/checkout@v4.2.0
```

Background

- GitHub Actions
 - Continuous Integration system
 - Reusable components called "Actions"
 - Versioned using git refs (*branch name*, *git tag*, *commit sha*)
 - Fetched at runtime
- Risks
 - Branch names and git tags are mutable (*ref confusion*)

Background

- GitHub Actions

- Continuous Integration system
- Reusable components called "Actions"
- Versioned using git refs (*branch name*, *git tag*, *commit sha*)
- Fetched at runtime

- Risks

- Branch names and git tags are mutable (*ref confusion*)
- Network commits can be used (*imposter commit*)

Background

- GitHub Actions

- Continuous Integration system
- Reusable components called "Actions"
- Versioned using git refs (*branch name*, *git tag*, *commit sha*)
- Fetched at runtime

- Risks

- Branch names and git tags are mutable (*ref confusion*)
- Network commits can be used (*imposter commit*)
- SHA1 hash collisions ([SHAttered](#), [SHAmbles](#))

Background

- GitHub Actions

- Continuous Integration system
- Reusable components called "Actions"
- Versioned using git refs (*branch name*, *git tag*, *commit sha*)
- Fetched at runtime

- Risks

- Branch names and git tags are mutable (*ref confusion*)
- Network commits can be used (*imposter commit*)
- SHA1 hash collisions ([SHAttered](#), [SHAmbles](#))
- Transitive and unpinnable actions

Tool Description

- Proper (SHA256) checksums for your GitHub Actions
- Better guarantees about what your CI is running
- Build using the libraries behind `go.sum`

ghasum / .github / workflows /

ericcornelissen Enable CodeQL scan for GitHub Actions

Name

- ..
- audit.yml
- check.yml
- codeql.yml
- gha.sum**
- ghasum.yml
- publish.yml
- semgrep.yml

ghasum / .github / workflows / gha.sum

ericcornelissen Enable CodeQL scan for GitHub Actions

Code Blame Executable File · 8 lines (7 loc) · 465 Bytes

```
1 version 1
2
3 actions/checkout@v4.2.0 e6ng7MJdyAPkTZ/6d/plZK2YhZRzJZvxhYAPUPpNAzc=
4 actions/setup-go@v5.3.0 vrKoUve8ZdSxhp4xwhswMTtCbXF6FZMic5MAm8uYduw=
5 github/codeql-action@v3.28.5 JbM1HEHSq9iqgLDWTXaWDK56mcCg5XB2iHkcxDHY1zI=
6 ncipollo/release-action@v1.15.0 4vkt9ENDRb/d8UYy0p878U4LRCcnasx8PeGPmXdt05E=
7 stefanzweifel/git-auto-commit-action@v5.0.0 t2VeG9180CmZ5/cmxxvkFkN6iWoWs0JlaJ2V8rp1HDqY=
8 tibdex/github-app-token@v2.1.0 ZNSBo6XSE0yxS8IkHEkVtUC9MkEeXTcLXpMLl6zAmCs=
```

Tool Benefits

- Checksums for branch and tag refs
- Network commits are disallowed
- Stronger checksum algorithm

Demo

Roadmap

- Support checking integrity during CI runs ([#4](#))
- Configurable hash algorithm ([#5](#))
- Transitive pinning for composite Actions ([#49](#) → [#209](#))
- Update checksums when updating Actions ([#9](#))

Roadmap

- Support checking integrity during CI runs ([#4](#))
- Configurable hash algorithm ([#5](#))
- Transitive pinning for composite Actions ([#49](#) → [#209](#))
- Update checksums when updating Actions ([#9](#))
- Suggestions...? Open an issue! *(after checking for duplicates)*

Takeaways

- `ghasum` > commit hash > tag ref > branch ref
 - [Immutable actions?](#)
- Checksums require configurable hashes
 - See also [npm/rfcs#757](#)
- Trust?
 - Checksum: today is the same as yesterday
 - Reproducible: I have the same as you
 - github.com/ericcornelissen/reproducing-actions

`ghasum` can be adopted today (but it's a bit rough)



ghasum

github.com/chains-project/ghasum

Eric Cornelissen (ericco@kth.se)



This work is licensed under a
Creative Commons Attribution 4.0 International License (CC BY 4.0)