



CI/CD with GitHub Actions

DevOpsCon London 2021 04 21



Lothar Schulz

CTO AIVITEX

lotharschulz.info

github.com/lotharschulz

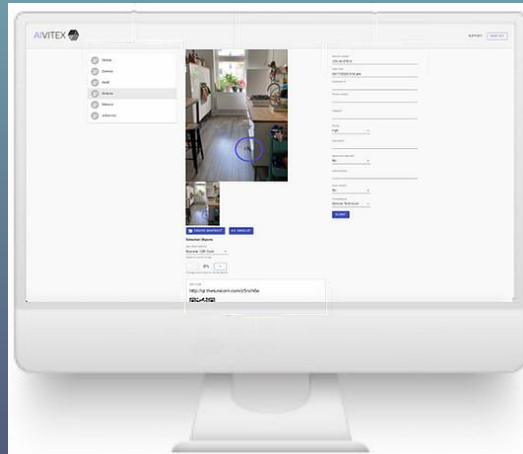
speakerdeck.com/lothar

[@lothar_schulz](https://twitter.com/lothar_schulz)

lnkd.in/in/lotharschulz



AI VITEX



GitHub Actions Workflow Automation



GitHub Actions Built-in CI/CD



What are GitHub Actions?

With GitHub Actions, workflows and steps are just code in a repository, so you can create, share, reuse, and fork your software development practices.



Deploy to Amazon ECS

Deploy a container to an Amazon ECS service powered by AWS Fargate or Amazon EC2.



[Set up this workflow](#)

```
# Build a docker container and
# push it to ECR so that it can
# be deployed to ECS.
```

 actions/starter-workflows

Build and Deploy to GKE

Build a docker container, publish it to Google Container Registry, and deploy to GKE.



[Set up this workflow](#)

```
# Set up docker to authenticate
# via gcloud command-line tool.
gcloud auth configure-docker
```

 actions/starter-workflows

Deploy Node.js to Azure Web App

Build a Node.js project and deploy it to an Azure Web App.



[Set up this workflow](#)

```
# Build and test the project, then
# deploy to Azure Web App.
npm install
```

 actions/starter-workflows

✓ build-node-versions (12.x)

✓ build-node-versions (14.x)

✓ build-node-versions (15.x)

✓ firebase-dev-deploy

dev_ci_cd.yml

on: push

Matrix: build-node-versions

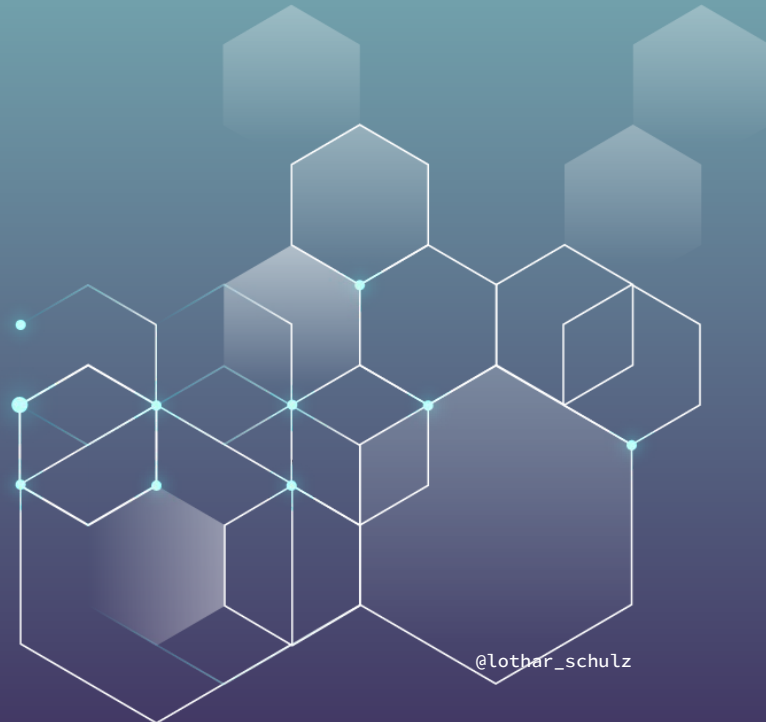
✓ 3 jobs completed

Show all jobs

✓ firebase-dev-deploy

2m 25s

Open Source



Community Resources

GitHub Tools and Management

- [Declaratively setup GitHub Labels](#)
- [Action to sync GitHub labels in the declarative way](#)
- [Add releases to GitHub](#)
- [Publish a docker image to Dockerhub](#)
- [Create an issue using content from a file](#)
- [Publish GitHub Releases with Assets](#)
- [GitHub Project Automation+ - Automate GitHub Project cards with any webhook event.](#)
- [Run GitHub Actions Locally with a web interface](#)
- [Run GitHub Actions Locally in Terminal](#)
- [Build and Publish Android debug APK](#)
- [Generate sequential build numbers for GitHub Actions](#)
- [Push Git changes to GitHub repository without authentication difficulties](#)
- [Generate release notes based on your events](#)
- [Create a GitHub wiki page based on the provided markdown file](#)
- [Label your Pull Requests auto-magically \(using committed files\)](#)
- [Add Label to your Pull Requests based on the author team name](#)
- [Manually trigger your GitHub Actions from a UI](#)
- [Get a list of file changes with PR/Push](#)
- [Use private actions in any workflow](#)
- [Label Your Issues Using the Issue's Contents](#)
- [Rollback a GitHub Release](#)
- [Lock Closed Issues and Pull Requests after a Period of Inactivity](#)
- [Get Commit Difference Count Between Two Branches](#)

Collection of Actions

- [Use HashiCorp's Terraform](#)
- [GitHub Actions for Yarn 1](#)
- [GitHub Actions for Yarn 2](#)
- [GitHub Actions for Golang](#)
- [GitHub Actions for R and accompanying #rstats package](#)
- [GitHub Actions for WordPress](#)
- [GitHub Actions for Composer](#)
- [GitHub Actions for Flutter](#)
- [GitHub Actions for PHP](#)

github.com/sdras/awesome-actions#community-resources

Open Source Projects using GitHub actions

(incomplete list)

- <https://github.com/gatsbyjs/gatsby/tree/master/.github/workflows>
- <https://github.com/hakimel/reveal.js/blob/master/.github/workflows/js.yml>
- <https://github.com/twbs/bootstrap/blob/master/.github/workflows/test.yml>
- <https://github.com/microsoft/vscode/tree/master/.github/workflows>
- <https://github.com/facebook/create-react-app/tree/master/.github/workflows>
- <https://github.com/hakimel/reveal.js/blob/master/.github/workflows/js.yml>
- <https://github.com/babel/babel/tree/master/.github/workflows>
- <https://github.com/nodejs/node/tree/master/.github/workflows>
- <https://github.com/microsoft/TypeScript/tree/master/.github/workflows>
- <https://github.com/kubernetes/utils/tree/master/.github/workflows>
- <https://github.com/jonico/programmatic-runner-test/blob/master/.github/workflows/blank.yml>
- <https://github.com/corona-warn-app/cwa-testresult-server/tree/master/.github/workflows>
- <https://github.com/corona-warn-app/cwa-verification-portal/tree/master/.github/workflows>
- <https://github.com/corona-warn-app/cwa-testresult-server/tree/master/.github/workflows>
- <https://github.com/OWASP/owasp-masvs/tree/master/.github/workflows>

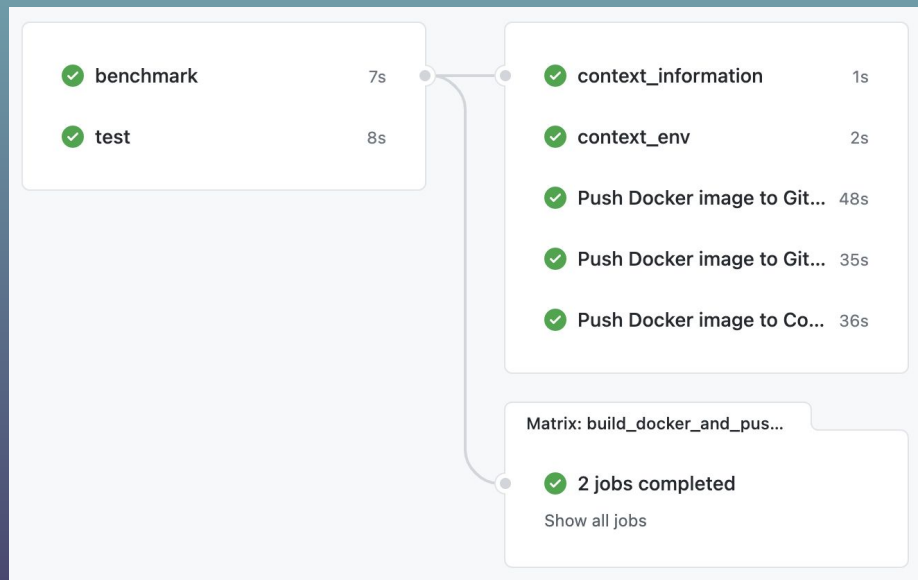


How To

Jobs

Jobs can run at the same time in parallel or be dependent on the status of a previous job and run sequentially.

```
build-and-dockerhub-push-if-linux:  
  needs: [benchmark, test]
```





Conditionals

```
if: matrix.os == 'ubuntu-18.04'
```

```
env:
```

```
  DOCKER_USERNAME: ${ secrets.DOCKER_USERNAME }
```

```
  DOCKER_PASSWORD: ${ secrets.DOCKER_PASSWORD }
```

```
run: |
```

```
  d=$(date +%Y-%m-%d)
```

```
  tag=$d-${ matrix.os }-${ github.sha }
```

```
  docker build -t lotharschulz/hello-github-actions:$tag .
```

```
  docker login -u ${DOCKER_USERNAME} -p ${DOCKER_PASSWORD}
```

```
  docker push lotharschulz/hello-github-actions:$tag
```



Matrix - Excludes

```
strategy:
  fail-fast: false
  matrix:
    os: [macOS-10.14,
ubuntu-18.04]
    goos: [linux, darwin]
    exclude:
      - os: macOS-10.14
        goos: linux
      - os: ubuntu-18.04
        goos: darwin
  runs-on: ${ matrix.os }
```



Matrix - Excludes

```
strategy:
  fail-fast: false
  matrix:
    os: [macOS-10.14,
ubuntu-18.04]
    goos: [linux, darwin]
  exclude:
    - os: macOS-10.14
      goos: linux
    - os: ubuntu-18.04
      goos: darwin
  runs-on: ${ matrix.os }
```

```
exclude:
  - os: macOS-10.14
    goos: linux
  - os: ubuntu-18.04
    goos: darwin
```



Matrix - Excludes

```
strategy:
  fail-fast: false
  matrix:
    os: [macOS-10.14,
ubuntu-18.04]
    goos: [linux, darwin]
  exclude:
    - os: macOS-10.14
      goos: linux
    - os: ubuntu-18.04
      goos: darwin
runs-on: ${ matrix.os }
```

```
exclude:
  - os: macOS-10.14
    goos: linux
  - os: ubuntu-18.04
    goos: darwin
```

```
include:
  - os: macOS-10.14
    goos: darwin
  - os: ubuntu-18.04
    goos: linux
```



Matrix

▼ Publish to Dockerhub and GitHub... 2

on: push

- ✓ benchmark
- ✓ test
- ✓ context_information
- ✓ context_env
- ✓ build_docker_and_push_to_doc...
- ✓ build_docker_and_push_to_doc...
- ✓ Push Docker image to GitHub P...
- ✓ Push Docker image to GitHub P...

build_docker_and_push_to_dockerhub_if_linux (macOS-10.15, darwin)

succeeded on Sep 18 in 9s

- > ✓ Set up job
- > ✓ Run actions/checkout@v1
- > ✓ builds the binary
- > ✓ Run actions/checkout@master
 - if linux build docker image and docker hub login as well as push
- > ✓ Post Run actions/checkout@master
- > ✓ Complete job

Matrix

▼ Publish to Dockerhub and GitHub... 2
on: push

- ✓ benchmark
- ✓ test
- ✓ context_information
- ✓ context_env
- ✓ build_docker_and_push_to_doc...
- ✓ build_docker_and_push_to_doc...
- ✓ Push Docker image to GitHub P...
- ✓ Push Docker image to GitHub P...

build_docker_and_push_to_dockerhub_if_linux (macOS-10.15, darwin)

succeeded on Sep 18 in 9s

- > ✓ Set up job
- > ✓ Run actions/checkout@v1
- > ✓ builds the binary
- > ✓ Run actions/checkout@master
 - if linux build docker image and docker hub login as well as push
- > ✓ Post Run actions/checkout@master
- > ✓ Complete job

Matrix

▼ Publish to Dockerhub and GitHub... 2

on: push

- ✓ benchmark
- ✓ test
- ✓ context_information
- ✓ context_env
- ✓ build_docker_and_push_to_doc...
- ✓ build_docker_and_push_to_doc...
- ✓ Push Docker image to GitHub P...
- ✓ Push Docker image to GitHub P...

build_docker_and_push_to_dockerhub_if_linux (ubuntu-20.04, linux)

succeeded on Sep 18 in 51s

- > ✓ Set up job
- > ✓ Run actions/checkout@v1
- > ✓ builds the binary
- > ✓ Run actions/checkout@master
- > ✓ if linux build docker image and docker hub login as well as push
- > ✓ Post Run actions/checkout@master
- > ✓ Complete job



Matrix - build only what you need

```
task testMatrix {
    project.afterEvaluate {
        def checkTasks = subprojects.collect {
            it.tasks.findByName("check")
        }.findAll { it != null }
        dependsOn(checkTasks)
        doLast {
            def checkTaskPaths = checkTasks
                .collect { it.path }
            println(JsonOutput.toJson(checkTaskPaths))
        }
    }
}
```

<https://github.com/testcontainers/testcontainers-java/blob/master/gradle/ci-support.gradle#L4-L18>
[faster parallel github builds](#)



Matrix - build only what you need

```
TASKS=$(./gradlew --no-daemon --parallel -q testMatrix)
echo $TASKS
echo "::set-output name=matrix::{\"gradle_args\":$TASKS}"
```

<https://github.com/testcontainers/testcontainers-java/blob/master/gradle/ci-support.gradle#L4-L18>
[faster parallel github builds](#)

Surprises

```
test:
  runs-on: ubuntu-18.04
  steps:
    - uses: actions/checkout@v1
    - uses: actions/setup-java@v1
      with:
        java-version: 11
    - uses: eskatos/gradle-command-action@v1
      with:
        arguments: test
    - name: test the code
```

GitHub Actions / `.github/workflows/main.yml`

failed 20 minutes ago in 0s

`.github/workflows/main.yml`

Invalid Workflow File

DETAILS

every step must define a `uses` or `run` key

Surprises

```
test:
  runs-on: ubuntu-18.04
  steps:
    - uses: actions/checkout@v1
    - uses: actions/setup-java@v1
      with:
        java-version: 11
    - uses: eskatos/gradle-command-action@v1
      with:
        arguments: test
# - name: test the code
```

GitHub Actions / .github/workflows/main.yml

failed 20 minutes ago in 0s

.github/workflows/main.yml

Invalid Workflow File

DETAILS

every step must define a `uses` or `run` key



Security

...

env:

```
GITHUB_CONTEXT: ${{ toJson(github) }}
```

run: |

```
REPO=$(echo $GITHUB_CONTEXT | jq -r '.repository')
```

...

<https://securitylab.github.com/research/github-actions-untrusted-input/>

Code





lotharschulz / hello-github-actions

Unwatch 1 Star 0 Fork 4

<> Code 1 Issues 0 Pull requests 2 Actions Projects 0 Wiki Security Insights Settings

hello github actions [Edit](#)

[Manage topics](#)

207 commits 7 branches 0 packages 0 releases 1 contributor

Branch: master New pull request Create new file Upload files Find file Clone or download

lotharschulz doc: Latest commit 0ac892f on 30 Dec 2019

.github	go with the exclude block	7 months ago
action	drop own docker cli action	11 months ago
.gitignore	make targets	11 months ago
CONTRIBUTING.md	doc:	3 months ago
Dockerfile	make targets	11 months ago
Makefile	linux and darwin traget os	7 months ago
README.md	docs:	4 months ago
build_test_benchmark_docker_build_push_and_shaking_finger...	actions screenshot	11 months ago
hello_test.go	unfail tests	11 months ago
hello_world.go	main comment	11 months ago
screenshot2019-08-23--12.17.35.png	v2 screenshot	7 months ago

README.md

GitHub Actions

Self Hosted & Awesome Runners

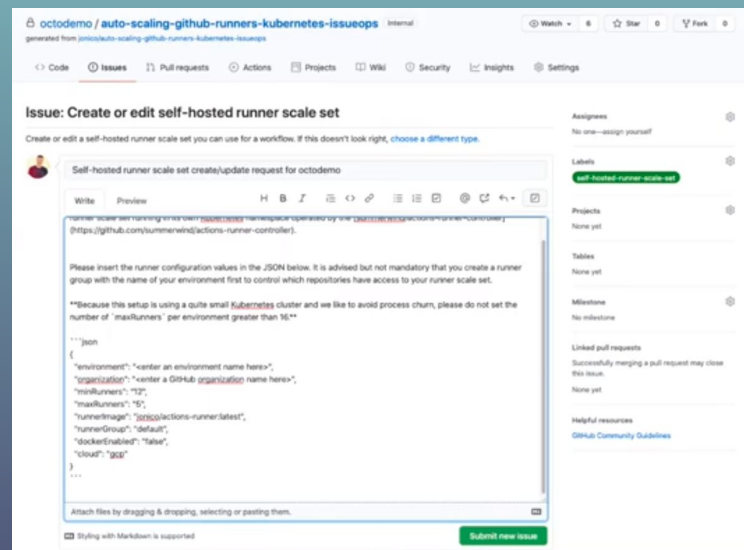


<https://github.com/jonico/awesome-runners>
lotharschulz.info/2019/12/09/github-action-self-hosted-runners-on-aws-incl-spot-instances

Issue Ops

<https://github.com/ionico/auto-scaling-github-runners-ec2-issueops>

<https://github.com/ionico/auto-scaling-github-runners-kubernetes-issueops>





There is more

Core concepts

Encrypted secrets

Packages container registry supports github_token



There is more

Contexts available on run time

Triggered by own events

Package manager and gh docker registry integrated



There is more

Run github actions locally

Organization Workflows

first-issue-greeter & github-workflow-sync



**I am sure you have
questions.**