GitHub Actions CI/CD workflows

CONCEPTS

Workflows live in .github/workflows/*.yml; each file holds jobs, each job runs steps on one fresh runner.

Workflow one YAML file, triggered by events
Job own runner, parallel unless needs
Step run: command or uses: action

TRIGGERS

`on: push`
Run on pushes

`on: pull_request`
Run on pull requests

`on.push.branches: [main, 'release/**']`
Only these branches

`on.push.tags: ['v*']`
Run on version tags

`on.<event>.paths: ['src/**']`
Only when these files change

`on.workflow_dispatch`
Allow manual runs

`on.schedule: - cron: '0 3 * * 1'`
Run on a cron schedule (UTC)

JOBS

`jobs.<id>.runs-on: ubuntu-latest`
Choose the runner

`needs: [<job>, <job>]`
Wait for other jobs

`if: github.event_name == 'push'`
Condition on a job or step

`if: always()`
Run even after failure

STEPS

`- uses: <owner>/<repo>@<ref>`
Run an action

`with: { <input>: <value> }`
Pass inputs to an action

`- run: <command>`
Run a shell command

`run: |`
Multi-line script

STEPS (cont.)

`id: <step_id>`
Name a step to read its outputs

`env: { <VAR>: <value> }`
Environment for a step

MATRIX & CONTAINERS

`strategy.matrix.<key>: [a, b]`
One job per value

`${{ matrix.<key> }}`
Read the current value

`strategy.fail-fast: false`
Let other legs finish

`services.<id>.image: <image>`
Sidecar such as a database

EXPRESSIONS & CONTEXTS

`${{ <expression> }}`
Evaluate an expression

`github.ref / github.ref_name`
Full ref / short branch or tag

`needs.<job>.outputs.<name>`
Output of a needed job

`steps.<id>.outputs.<name>`
Output of an earlier step

DATA & SECRETS

`secrets.<NAME>`
Read a repository secret

`secrets.GITHUB_TOKEN`
Automatic per-run token

`echo "k=v" >> "$GITHUB_OUTPUT"`
Set a step output

PERMISSIONS & CONCURRENCY

`permissions: contents: read`
Least-privilege GITHUB_TOKEN

REUSE, CACHE & ARTIFACTS

`uses: actions/cache@v4`
Cache dependencies

`uses: actions/upload-artifact@v4`
Keep files from a run