

CI/CD 构建

构建

构建	构建	runner tag
构建 / 构建 / 构建 / 构建 / 构建	构建 job	构建 runner
构建	kaniko	构建 runner
<code>docker run</code> / <code>compose</code> 构建 Docker in Docker	DinD	<code>dind</code> 构建 runner

tags 构建

- 构建 runner 构建 tags 构建 job 构建 kaniko 构建 tags: [docker] 构建
- 构建 DinD 构建 tags: [dind] 构建 tag 构建 runner 构建 job 构建 Docker 构建
- 构建 runner 构建 runner 构建 tag 构建 tags: [myrunner] 构建
- 构建 runner 构建 "Run untagged jobs" 构建 tags 构建 job 构建

构建 job

“构建构建 job 构建 job
构建 stage 构建 script 构建 构建 job
= 构建 + 构建 + 构建

-  Docker daemon
-  `docker build`  kaniko / DinD 
-  Docker Hub / gcr.io / ghcr.io / quay.io / nvcr.io / registry.gitlab.com /
registry.k8s.io 

 / 

```
build:
  stage: build
  image: node:lts
  script:
    - npm ci
    - npm run build
  artifacts:
    paths: [dist/]
```



```
test:
  stage: test
  image: node:lts
  needs: [build]
  script:
    - npm ci
    - npm test -- --reporter=junit --outputFile=report.xml
  artifacts:
    when: always
    reports:
      junit: report.xml
```

 / 

```
lint:
  stage: test
  image: node:lts
  script:
```

```
- npm ci
- npx eslint .
```



```
package:
  stage: package
  image: alpine:latest
  needs: [build]
  script:
    - tar -czf myapp.tar.gz -C dist .
  artifacts:
    paths: [myapp.tar.gz]
```

“ package stage stages: [build, test, package, deploy] GitLab .pre / build / test / deploy / .post



deployment job

rsync scp sftp WebDAV kubectl
script

“ Token GitLab CI/CD
.gitlab-ci.yml

```
deploy:
  stage: deploy
  image: alpine:latest
  variables:
    GIT_STRATEGY: none
  environment:
    name: production
```

```
url: https://myapp.example.com
resource_group: production
rules:
  - if: $CI_COMMIT_BRANCH == "main"
    when: manual
before_script:
  - apk add --no-cache openssh-client rsync
  - mkdir -p ~/.ssh && chmod 700 ~/.ssh
  - install -m 600 "$SSH_PRIVATE_KEY" ~/.ssh/id_ed25519
  - install -m 644 "$SSH_KNOWN_HOSTS" ~/.ssh/known_hosts
script:
  - rsync -az --delete -e "ssh -i ~/.ssh/id_ed25519" dist/ deploy@my-server:/srv/myapp/
  - ssh -i ~/.ssh/id_ed25519 deploy@my-server 'cd /srv/myapp && docker compose up -d'
```

Settings → CI/CD → Variables

SSH_PRIVATE_KEY	File	File <code>\$SSH_PRIVATE_KEY</code> <code>install -m 600</code> <code>"\$SSH_PRIVATE_KEY" ~/.ssh/id_ed25519</code>
SSH_KNOWN_HOSTS	Variable File	ssh-keyscan my- server <code>StrictHostKeyChecking=no</code>
/ Token	Variable	Masked Protected job

- job 600 job
-
- protected branch + when: manual + environment + resource_group
- deploy token / deploy key PAT

kaniko

job registry Docker daemon

- `docker run / compose RUN --mount=type=secret`
- DinD runner
- `--cache-repo` registry
- `tag debug tag latest scratch`
shell CI
- `GoogleContainerTools/kaniko` 2025-06 v1.24.0 `martizih/kaniko`
`osscontainertools/kaniko`

```
build-image:
  stage: build
  image:
    name: martizih/kaniko:debug # tag shell
ghcr.io/osscontainertools/kaniko:debug
  entrypoint: [""]
  script:
    - mkdir -p /kaniko/.docker
    - |
      cat > /kaniko/.docker/config.json <<CONF

{"auths":{"${CI_REGISTRY}":{"username":"${CI_REGISTRY_USER}","password":"${CI_REGISTRY_PASSWORD}"}}}

CONF
- /kaniko/executor
  --context "${CI_PROJECT_DIR}"
  --dockerfile "${CI_PROJECT_DIR}/Dockerfile"
  --destination "${CI_REGISTRY_IMAGE}:${CI_COMMIT_SHORT_SHA}"
  --destination "${CI_REGISTRY_IMAGE}:latest"
  --snapshot-mode=redo
  --compressed-caching=false
  --cache=true
  --cache-repo="${CI_REGISTRY_IMAGE}/cache"
```

DinD

job Docker build / run / compose

- privileged runner user-namespace
- docker build / run / compose docker buildx binfmt_misc multi-arch / QEMU
- daemon job job registry /artifacts docker

```
build-and-test:
  stage: test
  tags: [dind] # ← Docker daemon runner
  image: docker:29-cli
  services:
    - name: docker:dind
      alias: docker
  variables:
    DOCKER_HOST: tcp://docker:2375
    DOCKER_TLS_CERTDIR: "" # 2375 job
  script:
    - docker build -t myapp:ci .
    - docker run --rm myapp:ci ./run-tests.sh
    - docker compose up -d --build && docker compose ps
```

runner

runner

GitLab runner

- Settings → CI/CD → Runners → New project runner

- `Tags` `myrunner` `job` `runner` "Run untagged jobs" `runner`
- `runner authentication token` `glrt-...`



runner

`Docker` `deb/rpm` `Kubernetes` `GitLab`

- <https://docs.gitlab.com/runner/install/>
- <https://docs.gitlab.com/runner/register/>

`--url` `https://git.nju.edu.cn/` `--token` `glrt-...` `--executor`



- `tags: [myrunner]` `job` `runner`
- GitLab → Runners `online` `job`



- `${CI_REGISTRY_IMAGE}` `=` `reg.nju.edu.cn/<namespace>/<project>`
- `/` `$CI_JOB_TOKEN` `registry` `Masked + Protected` `CI`
- `.gitlab-ci.yml` `--build-arg SECRET=...` `dind` `RUN --mount=type=secret` `kaniko`
- Docker Hub `Dependency Proxy`



- `tags: [dind]` → job `kaniko` Docker daemon `kaniko` runner
- `services: [docker:dind]` → `tcp://docker:2375`
- `kaniko` `martizih/kaniko:latest` → `kaniko` `scratch` `kaniko` `shell` CI `kaniko`
`kaniko` `martizih/kaniko:debug`
- `kaniko` `.gitlab-ci.yml` `kaniko` `--build-arg SECRET=...` `kaniko` →
`kaniko` CI/CD `kaniko` DinD `kaniko` `RUN --`
`mount=type=secret` `kaniko` `kaniko`

Revision #24

Created 2026-09-27 09:10:46 CST by Yao Ge

Updated 2026-09-27 10:29:10 CST by Yao Ge