Hadolint Dockerfile linter

START HERE

`hadolint Dockerfile`
Lint a Dockerfile

`-f json`
Machine-readable output

`hadolint - < Dockerfile`
Lint from stdin

`--trusted-registry` *`<host>`*
Allow only this registry

`--ignore DL3008`
Skip one rule

`.hadolint.yaml`
Project config file

`-t error`
Fail only on errors

`# hadolint ignore=DL3006`
Silence next line

Dockerfile file or stdin → **parse** → **DL rules** build best practices → **RUN lines** → **ShellCheck** SC rules on shell → **filter** → **Report** tty, json, sarif, ... → **threshold** → **Exit code** 0 or 1

CONCEPTS

Hadolint parses the Dockerfile into an AST, applies its own DLxxxx rules and runs ShellCheck (SCxxxx) on every RUN.

RUN IT

`hadolint` *`<Dockerfile>`*
Lint a file

`hadolint` *`<Dockerfile>`* *`<Dockerfile2>`*
Lint several files

`hadolint - < Dockerfile`
Read the Dockerfile from stdin

`docker run --rm -i hadolint/hadolint < Dockerfile`
Run without installing

Also published as ghcr.io/hadolint/hadolint; tags latest-alpine and latest-debian.

`podman run --rm -i docker.io/hadolint/hadolint < Dockerfile`
Same via Podman

`docker run --rm -i -v "$PWD/.hadolint.yaml:/.config/hadolint.yaml" hadolint/hadolint < Dockerfile`
Use a config in the container

`hadolint --version`
Show the version

`hadolint --help`
List all options

`hadolint -V` *`<Dockerfile>`*
Verbose log to stderr

`brew install hadolint`
Install on macOS

`scoop install hadolint`
Install on Windows

RULES AND SEVERITY

`--ignore` *`<RULE>`*
Ignore a rule (repeatable)

`--error` *`<RULE>`*
Raise a rule to error

`--warning` *`<RULE>`*
Set a rule to warning

`--info` *`<RULE>`*
Set a rule to info

`--style` *`<RULE>`*
Set a rule to style

RULES AND SEVERITY (cont.)

`--trusted-registry` *`<host>`*
Only allow FROM images from this registry

Repeatable; violations are rule DL3026.

`--require-label` *`<label>`*`:`*`<type>`*
Require a label with a value type

Types: text, url, semver, hash, rfc3339, spdx, email.

`--strict-labels`
Reject labels not in the schema

`--disable-ignore-pragma`
Ignore all inline ignore comments

FAILURE AND OUTPUT

`-t` *`<level>`* **`/ --failure-threshold`** *`<level>`*
Exit non-zero from this severity up

Levels: error, warning, info, style, ignore, none. Default is info. All findings are still printed.

`--no-fail`
Always exit 0

`-f` *`<format>`*
Choose the output format

`-f json`
JSON array of findings

`-f sarif`
SARIF for code scanning

`-f checkstyle`
Checkstyle XML

`-f codeclimate / -f gitlab_codeclimate`
Code Climate JSON

`-f gnu`
GNU-style file:line: messages

`-f sonarqube / -f junit / -f codacy`
Other CI report formats

`--no-color`
Plain text output

`--file-path-in-report` *`<path>`*
Override the path shown in reports

Applies to checkstyle, codeclimate, sonarqube, junit and gitlab_codeclimate.

INLINE PRAGMAS

`# hadolint ignore=`*`<RULE>`*
Ignore a rule for the next instruction

`# hadolint ignore=`*`<RULE1>`***`,`***`<RULE2>`**
Ignore several rules at once

`# hadolint global ignore=`*`<RULE>`*
Ignore a rule for the whole file

`# hadolint shell=`*`<shell>`*
Declare a non-POSIX shell

Example: powershell, so ShellCheck is not applied wrongly.

Put the pragma on its own line directly above the instruction it covers.

CONFIG FILE

`.hadolint.yaml`
Project config in the current directory

`-c` *`<file>`* **`/ --config`** *`<file>`*
Use an explicit config file

`ignored: [DL3008, DL3059]`
List ignored rules

`trustedRegistries: [docker.io]`
Allowed FROM registries

`failure-threshold: warning`
Set the threshold

`override: {error: [DL3010]}`
Change rule severities

`label-schema: {version: semver}`
Required labels and types

`format: json`
Default output format

`$XDG_CONFIG_HOME/hadolint.yaml`
Per-user fallback location

Also ~/.config/hadolint.yaml and ~/.hadolint.yaml; the first match is used, not merged.

`HADOLINT_IGNORE=`*`<RULES>`*
Ignore rules via environment

`HADOLINT_NOFAIL=1`
Never fail, via environment

COMMON RULES

`DL3006`
Tag the base image version

COMMON RULES (cont.)

`DL3007`
Do not use the latest tag

`DL3008`
Pin apt-get package versions

`DL3009`
Delete apt lists after installing

`DL3015`
Add --no-install-recommends

`DL3002`
Last USER should not be root

`DL3003`
Use WORKDIR, not cd

`DL3020`
Use COPY instead of ADD for files

`DL3059`
Merge consecutive RUN instructions

`DL4006`
Set pipefail before piping in RUN

`SC2086`
Quote variables (ShellCheck)

RECIPES

CI gate: fail on warnings and worse

```
hadolint -t warning Dockerfile
```

Project config

```
# .hadolint.yaml
ignored:
  - DL3008
trustedRegistries:
  - docker.io
  - ghcr.io
failure-threshold: warning
```

Lint all Dockerfiles in a repo

```
find . -name 'Dockerfile*' -print0 \
  | xargs -0 hadolint -f json > hadolint.json
```

Targeted pragma

```
# hadolint ignore=DL3008
RUN apt-get update && apt-get install -y curl
```