Hadolint Dockerfile linter

CONCEPTS

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

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

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

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

brew install hadolint
Install on macOS

RULES AND SEVERITY

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

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

RULES AND SEVERITY (cont.)

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

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

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

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

FAILURE AND OUTPUT

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

--no-fail
Always exit 0

-f *<format>*
Choose the output format

-f json
JSON array of findings

-f sarif
SARIF for code scanning

--no-color
Plain text output

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

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

CONFIG FILE (cont.)

ignored: [DL3008, DL3059]
List ignored rules

trustedRegistries: [docker.io]
Allowed FROM registries

failure-threshold: warning
Set the threshold

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

HADOLINT_IGNORE=*<RULES>*
Ignore rules via environment

COMMON RULES

DL3006
Tag the base image version

DL3007
Do not use the latest tag

DL3008
Pin apt-get package versions

DL3009
Delete apt lists after installing

DL3002
Last USER should not be root

DL3003
Use WORKDIR, not cd

DL4006
Set pipefail before piping in RUN

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
```