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

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

RULES AND SEVERITY

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

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

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

--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

ignored: [DL3008, DL3059]
List ignored rules

trustedRegistries: [docker.io]
Allowed FROM registries

failure-threshold: warning
Set the threshold

COMMON RULES

DL3006
Tag the base image version

DL3007
Do not use the latest tag

DL3008
Pin apt-get package versions