TFLint Terraform linter

CONCEPTS

TFLint checks Terraform code for mistakes terraform validate misses: bad instance types, deprecated syntax, unused declarations.

.tflint.hcl plugins and rules
↓ `tflint --init`
Plugins rulesets on disk
↓ `tflint`
Rules run on your .tf files
↓ `exit code`
Issues error / warning / notice

The terraform ruleset is bundled and on by default; cloud rulesets (aws, azurerm, google) are plugins you must declare and install.

Run tflint from the module directory, or pass --chdir: it reads .tf files and config from there, not from parent dirs.

SETUP

`brew install terraform-linters/tap/tflint`
Install with Homebrew

`tflint --version`
Show version and loaded plugins

`tflint --init`
Install plugins from the config

`tflint --recursive --init`
Install plugins for all directories

`docker run --rm -v $(pwd):/data -t ghcr.io/terraform-linters/tflint`
Run the container image

`export GITHUB_TOKEN=`*`<token>`*
Avoid the --init rate limit

RUNNING

`tflint`
Lint the current directory

`tflint --chdir=`*`<dir>`*
Lint a different directory

`tflint --recursive`
Lint each directory below here

`tflint --filter=`*`<file>`*
Only report issues in this file or glob

RUNNING (cont.)

`tflint --fix`
Apply automatic fixes

`tflint --call-module-type=`*`<all|local|none>`*
Choose which module calls to inspect

`tflint --help`
List all options

OUTPUT AND EXIT CODES

`tflint --format=compact`
One line per issue

`tflint --format=json`
Machine-readable output

`tflint --format=sarif`
SARIF for code scanning

`tflint --no-color`
Plain output

`tflint --force`
Exit 0 even if issues are found

`tflint --minimum-failure-severity=`*`<error|warning|notice>`*
Fail only at this severity or worse

Exit codes

Code	Meaning
0	No issues
1	Error while running
2	Issues found

RULES

`tflint --enable-rule=`*`<rule>`*
Enable a rule for this run

`tflint --disable-rule=`*`<rule>`*
Disable a rule for this run

`tflint --only=`*`<rule>`*
Run just this rule

CONFIG FILE

`tflint --config=`*`<file>`*
Use this config file

`tflint --config=$(realpath .tflint.hcl) --recursive`
Share one config across directories

CONFIG FILE (cont.)

Config lookup order

Order	File
1	`--config`
2	`$TFLINT_CONFIG_FILE`
3	`./.tflint.hcl`
4	`./.tflint.json`
5	`~/.tflint.hcl`
6	`~/.tflint.json`

plugin and rule blocks

```
plugin "aws" {
  enabled = true
  version = "0.4.0"
  source  = "github.com/terraform-linters/tflint-ruleset-aws"
}

rule "terraform_typed_variables" {
  enabled = true
}
```

Plugin version must be exact and without a leading v; constraints like >= 0.3 are not supported.

IGNORING ISSUES

Ignore one line

```
# tflint-ignore: <rule>
instance_type = "t1.2xlarge"
```

Ignore a whole file

```
# tflint-ignore-file: <rule>
```

tflint-ignore-file only works at the top of a file; inside a block it is an error. In .tf.json files use a "//" property.

MODULES AND VARIABLES

`tflint --var-file=`*`<file>`*
Load a tfvars file

`tflint --var='`*`<name>`*`=`*`<value>`*`'`
Set a variable

`tflint --ignore-module=`*`<source>`*
Skip a module by source

RECIPES

CI check with a report

```
tflint --init
tflint --recursive --format=sarif > tflint.sarif
# exit code 2 fails the job
```