Trivy Cheat Sheet

Installation

Trivy can be installed as a Docker image or standalone binary. See https://trivy.dev/latest/getting-started/installation/.

Global configuration flags

Flag	Description
`-c, --config <file>`	The path to a configuration file (default: `trivy.yaml`)
`-d, --debug`	Enable debug mode
`--help`	Show help for the current command
`--quiet`	Suppress progress bar and log output
`-v, --version`	Show version information

Scan targets

Command	Description
`trivy config <directory>`	Scan configuration files for misconfigurations
`trivy filesystem <path>`	Scan a local filesystem path
`trivy image <image>`	Scan a container image
`trivy kubernetes [<context>]`	Scan resources in a Kubernetes cluster
`trivy repository <path|url>`	Scan a local or remote Git repository
`trivy rootfs <rootdir>`	Scan a local root filesystem directory
`trivy sbom <path>`	Scan a SBOM file for vulnerabilities and licenses
`trivy vm <image>`	Scan a virtual machine image

Scanners

Name	Description
`vuln`	Detects known vulnerabilities in components
`misconfig`	Detects configuration issues in Docker, Kubernetes, Terraform, etc. files
`secret`	Scans for exposed secrets (keys, tokens, etc.)
`license`	Scans for licensing risks

Scan flags

Flag	Description
`--scanners <scanners>`	Comma-separated list of enabled scanners (vuln,misconfig,secret,license) (default: vuln,secret)
`--skip-dirs <dirs>`	Directories or glob patterns to skip
`--skip-files <files>`	Files or glob patterns to skip

Report flags

Flag	Description
`-f, --format <string>`	Output format (table, json, template, sarif, etc.)
`-o, --output <file>`	Output file (default: stdout)
`-s, --severity <severities>`	Comma-separated list of severities to display (default: `UNKNOWN,LOW,MEDIUM,HIGH,CRITICAL`)
`--compliance <report>`	Generate a compliance report (`docker-cis-1.6.0`, `k8s-nsa-1.0`, `k8s-cis-1.23`, etc.)
`--exit-code <code>`	Specify the exit code when vulnerabilities found

Kubernetes flags

Flag	Description
`--disable-node-collector`	Don't start the node-collector job in the cluster
`--include-namespaces <namespace>`	Limit scanning to the specified namespaces

Examples

```
# Scan a container image
trivy image alpine:3.12

# Scan the current directory for secrets
trivy filesystem --scanners secret .

# Scan Kubernetes manifests for misconfigurations
trivy config kubernetes/
```