



Trivy : Scanner de Vulnérabilités Cloud-Native



10 mai 2026



Mis à jour le 17 mai 2026



24 min de lecture



5133 mots

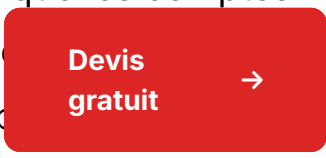


Guide entity-first 2026 sur Trivy : scanner de vulnérabilités open source par Aqua Security. Capacités scan (containers, filesystems, IaC, K8s, AWS, S3), bases vulnérabilités (Trivy DB, NVD, GHSA, OSV), Trivy Operator Kubernetes, intégrations CI/CD (GitHub Actions, GitLab, Jenkins), comparatif Gype, Snyk, Clair, Anchore, performances, faux positifs, cas DevSecOps shift-left, supply chain, runtime.



Trivy est le **scanner de vulnérabilités open source** le plus largement adopté de l'écosystème cloud-native, développé et maintenu par **Aqua Security** depuis 2019, distribué sous licence *Apache 2.0* et capable d'analyser en quelques secondes des images de conteneurs, des systèmes de fichiers, des dépôts Git, des manifestes Kubernetes, des modules Terraform, des templates AWS CloudFormation, des Do des charts Helm, des SBOM CycloneDX/SPDX, ainsi que les comptes AWS et clusters Kubernetes en production. En 2026, Trivy dépasse le Snyk sur GitHub et s'installe comme le scanner par défaut dans la plupart des pipelines CI/CD modernes (GitHub Actions, GitLab CI, Jenkins).

Réponse sous 24h



Actions, GitLab Security, Jenkins, CircleCI, Azure DevOps), supplantant les solutions historiques telles que Clair ou Anchore Engine grâce à son installation triviale (`brew install trivy` ou binaire statique de 60 Mo), sa base de vulnérabilités *Trivy DB* qui se rafraichit toutes les six heures, et son extension **Trivy Operator** qui industrialise la sécurité Kubernetes via des CRD (`VulnerabilityReport` , `ConfigAuditReport` , `ExposedSecretReport`). Ce guide entity-first détaille l'historique du projet, ses cas d'usage, son mode de scan, ses bases de vulnérabilités, la génération et l'analyse de SBOM, la détection de mauvaises configurations IaC, le secret scanning, la conformité licence, les intégrations avec GitHub Actions, le Trivy Operator, son positionnement face à Gype, Snyk, Clair et Anchore, ainsi que ses limites et cas d'usage DevSecOps.

À RETENIR

L'essentiel à retenir

Scanner all-in-one open source : Trivy analyse vulnérabilités, misconfigurations, secrets, licences et SBOM dans un seul binaire Go statique.

Couverture cloud-native complète : conteneurs OCI, filesystems, dépôts Cloud, Kubernetes, comptes AWS, Terraform, CloudFormation, Helm, Dockerfile, GitHub Actions.

Trivy DB : base de vulnérabilités agrégée (NVD, GHSA, OSV, advisories venant de Red Hat, Debian, Alpine, Ubuntu, Amazon, Photon), refresh toutes les 6 heures.

Trivy Operator Kubernetes : scan continu des workloads via CRD, intégration avec Prometheus, Falco, Defectdojo et OpenSearch.

Un projet cybersécurité ?
Réponse sous 24h

Devis
gratuit →

Réponse sous 24h

Devis
gratuit →