AYI NEDJIMI Consultants

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 p
Aqua Security. Capacités scan (containers, filesystems, IaC, K8s, AWS, SB
bases vulnérabilités (Trivy DB, NVD, GHSA, OSV), Trivy Operator Kubernet
intégrations CI/CD (GitHub Actions, GitLab, Jenkins), comparatif Grype, Sn
Clair, Anchore, performances, faux positifs, cas DevSecOps shift-left, supp
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 de images de conteneurs, des systèmes de fichiers, des dépôts Git, des manifestes Kubernetes, des modules Terraform, des templates AWS CloudFormation, des Doc des charts Helm, des SBOM CycloneDX/SPDX, ainsi que les comptes AWS et clust Kubernetes en production. En 2026, Trivy dépasse l **GitHub** et s' comme le scanner par défaut dans la plupart des pip ernes (GitH

Actions, GitLab Security, Jenkins, CircleCI, Azure DevOps), supplantant les solutio historiques telles que Clair ou Anchore Engine grâce à son installation triviale (`bre install trivy` ou binaire statique de 60 Mo), sa base de vulnérabilités *Trivy DB* r jour toutes les six heures, et son extension **Trivy Operator** qui industrialise la sécu Kubernetes via des CRD (`VulnerabilityReport` , `ConfigAuditReport` , `ExposedSecretReport`). Ce guide entity-first détaille l'historique du projet, ses ca de scan, ses bases de vulnérabilités, la génération et l'analyse de SBOM, la détect mauvaises configurations IaC, le secret scanning, la conformité licence, les intégra CD, le Trivy Operator, son positionnement face à Grype, Snyk, Clair et Anchore, ai 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 stati

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

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

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

Réponse sous 24h

Devis gratuit →