+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 01/06/2026

S'inscrire

Formation Artifact Registry

2 jours (14 heures)

Présentation

Un artifact registry centralise, versionne et sécurise vos artefacts (images Docker, packages, charts) pour fiabiliser les déploiements et accélérer les pipelines CI/CD. Il répond aux cas d'usage de promotion d'environnements, de traçabilité et de contrôle d'accès en entreprise.

Cette formation vous apprend à concevoir et opérer un registry comme composant clé de votre chaîne DevOps : organisation des dépôts, conventions de versioning, politiques de rétention, signatures et scans de vulnérabilités. Vous verrez comment intégrer le registry aux workflows Git, aux runners CI et aux clusters Kubernetes.

L'approche est résolument pratique, avec ateliers guidés et démos reproductibles : publication d'artefacts, configuration des permissions, mise en cache, promotion entre environnements et dépannage des erreurs courantes. Les livrables incluent des scripts/commandes, une checklist d'exploitation et un modèle de gouvernance (naming, ACL, lifecycle).

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Mettre en place un artifact registry et structurer les dépôts.
- Publier et consommer des images, packages et charts de façon industrialisée.
- Sécuriser avec RBAC, tokens, signatures et politiques de rétention.
- Intégrer le registry aux pipelines CI/CD et à Kubernetes.
- Diagnostiquer les problèmes de pull/push, cache, quotas et réseau.

Public visé

- Développeurs et développeuses
- Ingénieurs DevOps / SRE
- Administrateurs systèmes et plateformes
- Tech leads et architectes

Pré-requis

- Pratique des commandes Linux et du terminal
- Notions de Docker et d’images
- Connaissances de base en Git et CI
- Notions réseau (DNS, HTTP/HTTPS, proxy)

Pré-requis techniques

- PC avec 8 Go RAM minimum (16 Go recommandé)
- Linux, macOS, ou Windows avec WSL2
- Docker ou Podman installé, accès à un terminal
- Éditeur de code (VS Code, IntelliJ, etc.)
- Accès Internet et droits d’installation sur la machine

Programme de notre formation Artifact registry

[Jour 1 - Matin]

Prise en main d’Artifact Registry et des formats d’artefacts

- Rôles d’un registry : stockage, distribution, traçabilité et gouvernance des artefacts
- Types supportés : images Docker/OCI, Helm charts, packages npm, Maven, Python
- Modèle d’organisation : projets, régions, repositories, tags et digests
- Authentification : gcloud, helpers Docker, tokens et comptes de service
- Atelier pratique : créer un repository, builder une image, la tagger et la pousser (push) dans Artifact Registry

[Jour 1 - Après-midi]

Sécuriser l’accès et industrialiser l’usage (IAM, policies, CI/CD)

- Contrôle d’accès IAM : rôles, permissions minimales, séparation dev/ops
- Bonnes pratiques de nommage, versioning et immutabilité (tags vs digests)
- Consommation côté runtime : pull depuis GKE, VM, Cloud Run (principes et prérequis)
- Intégration pipeline : build, push, promotion entre environnements (dev/staging/prod)
- Atelier pratique : mettre en place un pipeline CI qui build et publie une image, puis déploie en utilisant le digest

[Jour 2 - Matin]

Gouvernance, nettoyage et optimisation des coûts

- Politiques de rétention : conserver N versions, gérer les tags “latest” et releases
- Nettoyage : suppression d’images non taggées, purge planifiée, prévention des dérives
- Stratégies multi-repos et multi-régions : latence, conformité, résilience
- Observabilité : audit des accès, suivi des pulls/pushs, alerting sur erreurs d’auth
- Atelier pratique : définir une politique de rétention et exécuter un nettoyage contrôlé avec validation des impacts

[Jour 2 - Après-midi]

Sécurité avancée : scanning, provenance et supply chain

- Vulnérabilités : lecture des rapports, criticité, priorisation et remédiation
- Signature et vérification : principes de confiance, contrôle avant déploiement
- Provenance : traçabilité build-to-deploy, métadonnées et attestations
- Gates de déploiement : bloquer les images non conformes (policy-as-code)
- Atelier pratique : activer le scanning, corriger une CVE, puis appliquer une règle de blocage sur images non signées

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des

séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.