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

Mis à jour le 20/06/2025

S'inscrire

Formation Harbor

3 jours (21 heures)

PRÉSENTATION

Notre formation Harbor vous apprendra à sécuriser, gérer et distribuer les images Docker et artefacts cloud-native au sein d'infrastructures d'entreprise. Il offre une alternative robuste aux registres publics comme Docker Hub, avec des fonctionnalités avancées de sécurité, de contrôle d'accès et de gouvernance.

Cette formation vous permettra de prendre en main l'outil de bout en bout : de son installation jusqu'à son intégration dans vos pipelines CI/CD. Vous apprendrez à créer des projets, gérer les utilisateurs via des rôles (RBAC), scanner automatiquement les images pour détecter les vulnérabilités, mettre en place des politiques de sécurité et répliquer vos artefacts entre environnements.

Votre équipe saura ainsi maîtriser les bonnes pratiques DevSecOps autour du stockage et de la distribution des images. Vous apprendrez à sécuriser le cycle de vie des conteneurs, à définir des règles d'immuabilité et de rétention, et à superviser l'état du registre grâce aux outils de monitoring intégrés.

Comme toutes nos formations, elle se déroulera sur la dernière version de l'outil : Harbor 2.13

OBJECTIFS

- Installer et configurer une instance de Harbor en environnement local ou cloud
- Organiser les dépôts via des projets et gérer les accès avec le modèle RBAC
- Scanner automatiquement les images pour détecter les vulnérabilités

PUBLIC VISÉ

- Ingénieurs DevOps
- Administrateurs système / cloud

- Responsables sécurité

Pré-requis

- Une bonne connaissance des concepts de conteneurisation (Docker)
- Des notions de base sur l’orchestration avec Kubernetes (pod, image, registre…)

Programme de notre Formation Spring Boot : Développer des microservices

Pourquoi un registre privé ?

- Évolution des registres : du Docker Hub public aux solutions on-premises
- Risques de sécurité et de conformité liés aux registres publics
- Besoins de performance : latence, limitation de bande passante, mise en cache
- Positionnement d’Harbor dans l’écosystème CNCF
- Cas d’usage typiques pour une équipe DevOps entreprise

Harbor en un clin d’œil

- Historique du projet : VMware ? CNCF (graduated)
- Vue d’ensemble de l’architecture micro-services
- Composants clés : Core, Registry, Portal, Trivy, Job Service, DB
- Parcours d’une requête docker push / pull dans Harbor
- Modes d’installation possibles : bundle Docker Compose ou Helm Chart

Installation mononœud et premiers pas

- Prérequis matériels & logiciels (Docker / Podman, 2 vCPU, SSL optionnel)
- Structure du fichier harbor.yml : hostname, admin pwd, certificats
- Lancement des conteneurs Harbor et vérification des services
- Découverte de l’interface Web et des menus principaux
- Atelier pratique : installer Harbor sur une VM locale et se connecter

Organisation par projets et contrôle d’accès (RBAC)

- Concept de projet : segmentation fonctionnelle et visibilité public/privé
- Rôles prédéfinis : Admin système, Project Admin, Developer, Guest
- Comptes utilisateurs locaux vs intégration LDAP / OIDC

- Création et utilisation des comptes robots pour la CI/CD
- Atelier pratique : créer deux comptes, attribuer les rôles et tester un push/pull

Sécurité des images et content trust

- Scanner Trivy : base CVE, déclenchement auto/manuel, seuils de sévérité
- Analyse des rapports de vulnérabilités et workflow de remédiation
- Signature d'images avec Notary / Cosign : principes et activation
- Blocage des pulls d'images non signées ou vulnérables (policy enforcement)
- Atelier pratique : pousser une image vulnérable, lancer un scan et corriger

Cycle de vie : rétention, immuabilité, quotas

- Règles de rétention de tags : garder n versions ou selon l'âge
- Immutabilité des tags de release pour garantir l'intégrité des builds
- Gestion des quotas par projet (GB, nombre d'artefacts)
- Garbage Collection : suppression physique des blobs et fenêtres de maintenance
- Audit & journaux : suivi des actions utilisateur et traçabilité

Réplication et scénarios multi-site

- Types de réplications : push, pull, bidirectionnelle
- Création d'endpoints : Harbor ? Harbor, Harbor ? Docker Hub, Harbor ? ECR
- Filtres d'inclusion (repository, tag) et planification
- Cas d'usage : DR, edge registry, déploiement multi-région
- Considérations de performance et de versionnement entre sites

Intégration dans la CI/CD et automatisation

- Schéma d'un pipeline : build ? scan ? push Harbor ? déploiement Kubernetes
- Utilisation des comptes robots et tokens dans Jenkins / GitLab CI
- Webhooks Harbor : déclencher un job ou un déploiement à chaque push
- GitOps & ArgoCD : tirer l'image validée depuis Harbor
- Supply Chain Security : SBOM, provenance, politiques « shift-left »

Exploitation, monitoring et bonnes pratiques

- Supervision des services : métriques Prometheus, alertes, logs
- Stratégie de sauvegarde : base PostgreSQL, stockage objets/blobs
- Plan de montée de version et tests de migration
- Gouvernance globale : checklist d'entreprise (sévérité CVE, quotas, naming)
- Ressources pour aller plus loin : documentation, communauté, roadmap Harbor

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.