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

Updated on 20/06/2025

Sign up

Harbor training

3 days (21 hours)

PRESENTATION

Our Harbor training course will teach you how to secure, manage and distribute Docker images and cloud-native artifacts within enterprise infrastructures. It offers a robust alternative to public registries like Docker Hub, with advanced security, access control and governance features.

This training course will enable you to get to grips with the tool from start to finish, from installation to integration in your CI/CD pipelines. You'll learn how to create projects, manage users via roles (RBAC), automatically scan images for vulnerabilities, set up security policies and replicate artifacts between environments.

This will enable your team to master DevSecOps best practices around image storage and distribution. You'll learn how to secure container lifecycles, define immutability and retention rules, and supervise registry status using integrated monitoring tools.

Like all our training courses, it will be run on the latest version of the tool: Harbor 2.13.

OBJECTIVES

- Install and configure a Harbor instance in a local or cloud environment
- Organize repositories via projects and manage access with the RBAC model
- Automatically scan images for vulnerabilities

TARGET AUDIENCE

- DevOps engineers
- System / cloud administrators

- Safety managers

Prerequisites

- Good knowledge of containerization concepts (Docker)
- Basic notions of orchestration with Kubernetes (pod, image, registry...)

Program of our Spring Boot Training: Developing microservices

Why a private register?

- Registry evolution: from public Docker Hub to on-premises solutions
- Security and compliance risks associated with public registers
- Performance requirements: latency, bandwidth limitation, caching
- Harbor's position in the CNCF ecosystem
- Typical use cases for an enterprise DevOps team

Harbor at a glance

- Project background: VMware ? CNCF (graduated)
- Overview of microservices architecture
- Key components: Core, Registry, Portal, Trivy, Job Service, DB
- Running a Docker push/pull request in Harbor
- Installation options: Docker Compose or Helm Chart bundle

Mononœud installation and first steps

- Hardware & software requirements (Docker / Podman, 2 vCPUs, SSL optional)
- harbor.yml file structure: hostname, admin pwd, certificates
- Harbor container launch and service verification
- Discover the Web interface and main menus
- Practical workshop: installing Harbor on a local VM and logging on

Project-based organization and access control (RBAC)

- Project concept: functional segmentation and public/private visibility
- Predefined roles: System Admin, Project Admin, Developer, Guest
- Local user accounts vs. LDAP / OIDC integration

- Creating and using robot accounts for CI/CD
- Practical workshop: create two accounts, assign roles and test a push/pull operation

Image security and content trust

- Trivy scanner: CVE base, auto/manual triggering, severity thresholds
- Vulnerability report analysis and remediation workflow
- Image signing with Notary / Cosign: principles and activation
- Blocking unsigned or vulnerable image pulls (policy enforcement)
- Practical workshop: push a vulnerable image, run a scan and correct

Lifecycle: retention, immutability, quotas

- Tag retention rules: keep n versions or according to age
- Immutability of release tags to guarantee build integrity
- Project quota management (GB, number of artifacts)
- Garbage Collection: physical removal of blobs and maintenance windows
- Audit & logs: tracking user actions and traceability

Replication and multi-site scenarios

- Replication types: push, pull, bidirectional
- Endpoint creation : Harbor ? Harbor, Harbor ? Docker Hub, Harbor ? ECR
- Inclusion filters (repository, tag) and planning
- Use cases: DR, edge registry, multi-region deployment
- Performance and versioning considerations between sites

CI/CD integration and automation

- Pipeline diagram: build ? scan ? push Harbor ? Kubernetes deployment
- Using bot and token accounts in Jenkins / GitLab CI
- Harbor Webhooks: trigger a job or deployment with every push
- GitOps & ArgoCD: pulling the validated image from Harbor
- Supply Chain Security: SBOM, provenance, shift-left policies

Operation, monitoring and best practices

- Service monitoring: Prometheus metrics, alerts, logs
- Backup strategy: PostgreSQL database, object/blob storage
- Upgrade plan and migration testing
- Global governance: company checklist (CVE severity, quotas, naming)
- Further resources: documentation, community, Harbor roadmap

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.

Training organization registered under number 11 75 54743 75. This registration does not imply government approval.
Ambient IT 2015-2025. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg