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

Updated on 06/01/2026

Sign up

Artifact Registry Training

2 days (14 hours)

Overview

An artifact registry centralizes, versions, and secures your artifacts (Docker images, packages, charts) to ensure reliable deployments and accelerate CI/CD pipelines. It addresses use cases such as environment promotion, traceability, and enterprise access control.

This training teaches you how to design and operate a registry as a key component of your DevOps pipeline: repository organization, versioning conventions, retention policies, signatures, and vulnerability scans. You'll learn how to integrate the registry with Git workflows, CI runners, and Kubernetes clusters.

The approach is firmly hands-on, featuring guided workshops and reproducible demos: publishing artifacts, configuring permissions, caching, promoting between environments, and troubleshooting common errors. Deliverables include scripts/commands, an operations checklist, and a governance template (naming, ACL, lifecycle).

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Set up an artifact registry and structure repositories.
- Publish and consume images, packages, and charts in a production-ready manner.
- Secure the system with RBAC, tokens, signatures, and retention policies.
- Integrate the registry with CI/CD pipelines and Kubernetes.
- Diagnose issues related to pull/push, cache, quotas, and networking.

Target Audience

- Developers
- DevOps / SRE engineers
- System and platform administrators
- Tech leads and architects

Prerequisites

- Familiarity with Linux commands and the terminal
- Basic understanding of Docker and images
- Basic knowledge of Git and CI
- Basic networking concepts (DNS, HTTP/HTTPS, proxy)

Technical prerequisites

- PC with at least 8 GB of RAM (16 GB recommended)
- Linux, macOS, or Windows with WSL2
- Docker or Podman installed, access to a terminal
- Code editor (VS Code, IntelliJ, etc.)
- Internet access and installation permissions on the machine

Our Artifact Registry Training Program

[Day 1 - Morning]

Introduction to Artifact Registry and artifact formats

- Roles of a registry: storage, distribution, traceability, and governance of artifacts
- Supported types: Docker/OCI images, Helm charts, npm packages, Maven, Python
- Organizational model: projects, regions, repositories, tags, and digests
- Authentication: gcloud, Docker helpers, tokens, and service accounts
- Hands-on workshop: creating a repository, building an image, tagging it, and pushing it to Artifact Registry

[Day 1 - Afternoon]

Securing access and scaling usage (IAM, policies, CI/CD)

- IAM access control: roles, least privilege, dev/ops separation
- Best practices for naming, versioning, and immutability (tags vs. digests)
- Runtime consumption: pulling from GKE, VM, Cloud Run (principles and prerequisites)
- Pipeline integration: build, push, promotion between environments (dev/staging/prod)
- Hands-on workshop: setting up a CI pipeline that builds and publishes an image, then deploys using the digest

[Day 2 - Morning]

Governance, cleanup, and cost optimization

- Retention policies: keep N versions, manage “latest” tags and releases
- Cleanup: deleting untagged images, scheduled purges, preventing data drift
- Multi-repository and multi-region strategies: latency, compliance, resilience
- Observability: access auditing, tracking pulls/pushes, alerting on auth errors
- Hands-on workshop: defining a retention policy and performing a controlled cleanup with impact validation

[Day 2 - Afternoon]

Advanced security: scanning, provenance, and supply chain

- Vulnerabilities: reading reports, severity, prioritization, and remediation
- Signature and verification: trust principles, pre-deployment checks
- Provenance: build-to-deploy traceability, metadata, and attestations
- Deployment gates: blocking non-compliant images (policy-as-code)
- Hands-on workshop: enable scanning, fix a CVE, then apply a blocking rule to unsigned images

Target Audience

This training is intended for both individuals and companies, large or small, seeking to train their teams in new advanced IT technologies or to acquire specific business knowledge or modern methodologies.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals regarding the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

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

Organization

The course alternates between theoretical input from the trainer, supported by examples and

reflection sessions and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.