AMBIENT-IT

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

Updated on 10/14/2026

Sign Up

GitLab Fundamentals Associate Certification Training

2 days (14 hours)

Overview

GitLab is a DevSecOps platform that brings together code management, collaboration, automation, and security in software development. With merge requests, agile planning, CI/CD pipelines, and security scans, GitLab supports teams throughout the entire delivery cycle.

Our GitLab Fundamentals Associate Certification Training will help you prepare for the official GitLab Fundamentals Associate certification by reinforcing the core skills assessed in the exam. You'll develop a structured approach to tackling the questions and scenarios presented.

You'll learn how to organize groups and projects, manage permissions, collaborate using branches and merge requests, and build a simple pipeline. The course also covers issues, tracking boards, and the principles of security by design.

By the end of the course, you'll be able to apply these features in a professional setting, diagnose a pipeline failure, and interpret a security report. Hands-on workshops and a practice exam will help you assess your progress and focus your final review before taking the official exam.

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

Objectives

- Organize groups, projects, and permissions in GitLab
- Implement a collaborative workflow using branches and merge requests

- Plan and track tasks using issues, labels, and boards
- Set up and troubleshoot a simple CI/CD pipeline
- Enable security scanning and interpret the results
- Assess your readiness for the GitLab Fundamentals Associate certification with a practice exam

Target Audience

- Software developer
- DevOps engineer
- DevSecOps engineer
- QA Engineer
- Technical Project Manager

Requirements

- Knowledge of the application development and delivery lifecycle
- Basic familiarity with Git, including commits and branches
- Comfort working with a terminal and handling configuration files
- Ability to understand technical documents written in English

Technical Prerequisites

- Computer with 8 GB of RAM recommended, running Windows 11, macOS, or Linux
- A recent stable version of Firefox or Chrome, with an Internet connection that supports the training services
- Git 2.x client and Visual Studio Code editor installed, or an equivalent environment validated prior to the session
- GitLab account with access to a learning environment, the necessary permissions, and a working runner for the workshops
- GitLab University account for exam registration, with access credentials verified prior to the exam

Curriculum for our GitLab Fundamentals Associate training

[Day 1 - Morning]

Project Organization and Planning

- Scope of the GitLab Fundamentals Associate Certification Training, skills assessed, and initial assessment
- DevSecOps Principles and GitLab’s Role in the Software Development Lifecycle
- Organizing groups, subgroups, and projects; visibility and permission inheritance
- Issue management, labels, and milestones; assigning responsibilities and tracking boards

- Collaborative documentation using the wiki, presentation files, and links between work items
- Hands-on Workshop: Structuring a project space, assigning roles, and organizing a set of tasks in a tracking board.

[Day 1 – Afternoon]

Code management and collaboration

- Review of Git operations: cloning, commits, synchronization, and viewing the history
- Branch and tag management, protecting the main branch, and choosing a collaborative workflow
- Creating merge requests, comparing changes, and linking to issues
- Organizing code reviews, providing feedback, resolving discussions, and approving changes based on permissions
- Resolving merge conflicts and analyzing representative collaboration scenarios the exam
- Hands-on workshop: Making a change on a branch, opening a merge request, conducting a review, and resolving a conflict before merging.

[Day 2 - Morning]

Building and troubleshooting pipelines

- Distinction between continuous integration, continuous delivery, and continuous deployment
- Structure of the .gitlab-ci.yml file, YAML syntax, jobs, stages, and scripts
- How runners work, runtime images, and job support requirements
- Using CI/CD variables, trigger rules, and best practices for managing secrets
- Distinction between artifacts and cache, reading logs, and troubleshooting common failures
- Hands-on workshop: Building a build and test pipeline, retaining an artifact, and fixing a job that intentionally fails.

[Day 2 - Afternoon]

Built-in Security and Final Preparation

- Principles of built-in security and the distinction between SAST, DAST, dependency analysis, and secret detection
- Enabling a SAST scanner with a CI/CD model and identifying features that depend on the subscription
- Reading security reports, severity levels, and tracking a fix within the project workflow
- View project and pipeline metrics to track activity and identify recurring failures recurring
- Exam preparation strategy, analysis of distractor options, time management, and study planning

- Hands-on workshop: Add a SAST analysis to the end-to-end project, interpret the report, and then conduct an original mock exam with annotated corrections and individual feedback.

Target Companies

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 industry knowledge or modern methodologies.

Entry-Level Assessment

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 level across various types of technologies, as well as their expectations and personal goals for 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 operation of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

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

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg