AMBIENT·IT

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

Updated 10/10/2024

Sign up

Keycloak training

2 days (14 hours)

PRESENTATION

Our Keycloak training course will help you secure access to your applications. Keycloak is a complete and powerful open-source Identity and Access Management (IAM) solution developed by RedHat.

In this course, you'll learn how to use Keycloak to manage authentication and authorization for your various applications. You'll learn how to control access to resources based on each user's credentials and authorizations. Key benefits of Keycloak include :

- An adaptable system that can handle an almost infinite number of accounts
- Integration of SAML, OAuth 2 and OpenID security protocols
- A regularly updated system for optimum protection
- A large, active community

Our Keycloak training course, which alternates 60% practice and 40% theory, will introduce you to the tool and the different ways of protecting your applications, and we'll go into more detail on tokens, configuration and authorization management on Keycloak.

No prior knowledge of security or complex authentication protocols is required: Keycloak offers high-level integration, so anyone can use it to secure their own applications and systems.

Our Keycloak training course will be based on the latest version of the tool, Keycloak 26.

OBJECTIVES

- Create an effective identity and access management architecture with Keycloak
- Understand the different security protocols and when/how to use them
- How to design and configure authorizations
- Install and configure Keycloak for production use

- Monitor application usage and analyze authentication errors
- Integrate Keycloak with existing directories

TARGET AUDIENCE

- Developers
- Directors
- Cybersecurity managers and experts

Prerequisites

- Good knowledge of Windows and Linux/UNIX
- Good TCP/IP skills
- Good command of HTTP
- Knowledge of software architecture
- Test My Knowledge

Software requirements

- Have Java installed
- Docker Desktop or Podman installed on your PCs

Recommendations for pre- and post-course reading

- "Keycloak - Identity and Access Management for Modern Applications" by Stian Thorgersen. This book is a truly comprehensive guide to Keycloak
- "Mastering Identity and Access Management with Microsoft Azure" by Jochen Nickel. This book provides an introduction to identity and access management and includes a section on Keycloak.
- Official Keycloak documentation
- You can also watch this introductory video to Keycloak

OUR KEYCLOAK TRAINING PROGRAM

Introduction to identity and access management Introduction

to Keycloak

- Keycloak features at a glance

- Keycloak technical architecture

User management in Keycloak

- Creating and managing users in Keycloak
- User roles and attributes
- Define administrative permissions for user accounts

User organization via groups

- Creating groups
- Assigning members to groups

Integration of existing directories

- Active Directory / LDAP integration
- LDAP attribute mapping

Identity management in Keycloak // Authentication with SSO

- Introduction to authentication standards
- SSO integration methods for applications
- Token and session management
- Integration with external security providers

Strengthening Keycloak's security

- Password policies and requirements
- Multi-factor authentication (MFA) and other security measures
- Best practices for securing your Keycloak installation
- Audit and compliance check of your Keycloak installation

Troubleshooting Keycloak

- Common problems and errors in Keycloak
- Techniques for diagnosing connection problems

Complementary module (+1 day)

HANDS-ON WORKSHOPS

- Lab 1: Authorization workflow in action
- Lab 2: Resource server
- Lab 3: Customer (authentication code)
- Lab 4: Customer (customer identification information)
- Lab 5: SPA customer (Authz code with PKCE)
- Lab 6: Authorization (AuthZ)
- Lab 7: Fine-grain authorization (Restrict scope)
- Lab 8: The Gatekeeper

BONUS LABS

- Demo/Lab 8: Multi-tenant resource server
- Demo/Lab 9: Resource server with Micronaut
- Demo/Lab 10: Resource server with Quarkus
- Lab 11: Testing JWT Auth&Authz
- Lab 12: JWT test server
- Lab 13: Keycloak test containers

Companies concerned

This training 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.