Ambient IT
128 Boulevard Macdonald
75019 Paris

Mail : formation@ambient-it.net
Tél : +33 (0)1 40 34 11 53

AMBIENT-IT

Training Keycloak

Duration 2 days (14 hours)

PRESENTATION

Keycloak is the most complete and powerful open-source Identity and Access Management (IAM) developed by RedHat, and it’s widely used and trusted by many companies.

In this training, we'll explore most of the Keycloak capabilities and features that help you secure your applications and services.

You'll discover how you can easily configure and set-up authentication for modern (and also legacy) applications with different technologies, enable two-factor authentication, integrate with external user registries like LDAP, delegate authentication to other identity providers, and a lot of other cool and useful features Keycloak brings to the table.

No previous knowledge on security and complex authentication protocols : Keycloak provides a high level integration so anyone and everyone can use it to secure their own applications and systems.

Our Keycloak training will be based on the latest version of the tool, Keycloak 12.

OBJECTIVES

- Building 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

INTENDED PUBLIC

- Developers
- Software architects
- Project managers
- Software Integrators

Prerequisites

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

PROGRAM OF OUR KEYCLOAK TRAINING

Part 1 : Introduction and Concepts

- Keycloack architecture and prerequisites
- Authentication workflows
- Token usage and lifecycle
- Configuring Roles and Permissions
- Using external identity providers
- Multi-tenancy with Keycloack
- Multi-factor authentication (MFA) using OTP

Part 2 : Hands-On Workshops

Hands-On Labs :

- Lab 1 : Authorization Grant Flows in Action
- Lab 2 : Resource Server
- Lab 3 : Client (Auth Code)
- Lab 4 : Client (Client-Credentials)
- Lab 5 : SPA Client (Authz Code with PKCE)
- Lab 6 : Authorization (AuthZ)
- Lab 7 : Fine-grained Authorization (Limiting the 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 Testing Server
- Lab 13 : Keycloak Testcontainers

Companies concerned

This training is intended for companies, small or large, wishing to train their teams to a new advanced computer technology.

Pedagogical methods

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

Organization

The course alternates theoretical contributions from the trainer supported by examples and reflection sessions, and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to verify the correct acquisition of skills.

Sanction

A certificate of course completion will be given to each trainee who will have followed the whole training.