AMBIENT-IT

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

Updated 05/03/2024

Sign up

Advanced Keycloak training

2 days (14 hours)

PRESENTATION

Simply secure your applications with the open-source Keycloak tool. With Keycloak, you can prevent unauthorized access and protect yourself against cyber attacks.

Created and updated by Red Hat, the tool supports three authentication protocols: SAML, OAuth 2 and OpenID.

Keycloak's many features include full support for SSO (Single Sign-On and Single Sign-Out), a user identity and access manager for creating a user database with customized roles and groups, and use of LDAP and Active Directory.

Our advanced Keycloak training course will teach you how to use Keycloak in an advanced way, with a presentation of the keycloak logger, user storage federation, client scope and authorization management.

Our advanced Keycloak training course will introduce the latest version of the tool, Keycloak 24.

OBJECTIVES

- Control the lifecycle of access and refresh tokens
- Configure and implement different authorization strategies
- Ensure the security of sensitive applications with Keycloak in compliance with the FAPI standard
- Use Keycloak's REST administration APIs for advanced authorization management

TARGET AUDIENCE

- Developers
- Technical architects

- Project managers
- Directors

Prerequisites

- Ideally, you should have taken our Keycloak training course.
- Knowledge of safety protocol
- Have already used Keycloak
- Good knowledge of Windows and Linux/UNIX
- Good TCP/IP skills
- Good command of HTTP
- Knowledge of software architecture

Software requirements

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

OUR ADVANCED KEYCLOAK TRAINING PROGRAM

Advanced use of OAuth tokens

- Understanding the life cycle
  - Access tokens
  - Refreshment tokens
- Configure Keycloak to generate/validate offline_access tokens
- Implementing exchange_token

Fine-tuning authorizations

- Protocol reminder
  - OAuth 2.0
  - OpenID Connect
- Understand the concepts of roles, permissions and policies in Keycloak
- Configure and implement different authorization strategies with Keycloak
- Delegate authorization management to the user with the UMA 2.0 standard

Secure sensitive applications with Keycloak

- Introduction to FAPI (Financial-grade API) and security requirements
- Implementing FAPI requirements in Keycloak
- Establish automated security tests for authorization mechanisms

Implementing Keycloak's REST Admin APIs

- Keycloak REST API presentation
- Testing the most frequently used requests via REST APIs

Keycloak customization

- Customize login page and email templates
- Configure custom authentication flows
- Extend Keycloak's functionality with SPI (Service Provider Interfaces)

Complementary module (+1 day)

Customer scope

- Presentation of scopes and claims
- The protocol
- Linking the customer scope with the customer
- Permissions
- Using scopes and claims
- Authentication with phone number
- Keycloak generator for scope evaluation

Advanced authorization management

- Understanding UMA in detail with Keycloak
- Using permissions
- Approval or revocation
- Access the UMA using the REST API
- Authorization services
- Evaluating and testing policies
- Strengthening policies

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 enrolment is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and objectives.

This questionnaire also enables us to anticipate any connection or internal security problems (intra-company or virtual classroom) that could be problematic for the follow-up and smooth running of the training session. This questionnaire also enables us to anticipate any connection or internal security difficulties within the company (intra-company or virtual classroom) that 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.