Updated 02/04/2025

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 SSO support (Single Sign-On and Single Sign-Out), 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 26.1.

OBJECTIVES

- Master the configuration and use of advanced tokens
- Install and configure Keycloak for production use
- Configure and implement different authorization strategies
- Use Keycloak's REST administration APIs for advanced authorization management
- Ensure the security of sensitive applications with Keycloak in compliance with the FAPI standard
- Customize Keycloak to suit your branding

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
- Test My Knowledge

Software requirements

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

OUR ADVANCED KEYCLOAK TRAINING PROGRAM

Advanced use of OAuth tokens

- Configure Keycloak to generate/validate offline_access tokens
- Implementing exchange_token

ADVANCED CONFIGURATION OF A KEYCLOAK CLIENT

- Keys & Credentials
- Advanced options

ADVANCED KINGDOM CONFIGURATION

- General configuration
- Events
- Location
- User profile & registration

TECHNICAL ARCHITECTURE (FOR PRODUCTION)

- Best practices for securing your Keycloak installation
- Multi-environment management
- DB
- Monitoring

KEYCLOAK REST ADMIN API IMPLEMENTATION

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

IMPLEMENTATION OF FINE-GRAINED AUTHORIZATIONS

- Understand the concepts of roles, permissions and policies in Keycloak
- Configure and implement different authorization strategies with Keycloak
- Understanding UMA with Keycloak
- Delegate authorization management to the user with the UMA 2.0 standard
- Access the UMA using the REST API

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

KEYCLOAK CUSTOMIZATION

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

ADDITIONAL MODULES: MODULE 1

(+0.5 day)

- Authentication with phone number
- Approval or revocation
- Evaluating and testing policies
- Strengthening policies

MODULE 2 (+0.5 day) :

- CUSTOM LAB (on request)

Companies concerned

This 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, 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.