Publication date : 02/05/2024

Course : Keycloak, implementation

Practical course - 4d - 28h00 - Ref. LDC
Price : 2890 CHF E.T.

4,3 / 5

This hands-on course introduces Keycloak, the open source identity and access management (IAM) solution associated with the implementation of SAML 2 standards. This course will enable you to effectively install, configure and monitor Keycloak in an enterprise context.

Teaching objectives

At the end of the training, the participant will be able to:

- Create a Keycloak instance
- Master Keycloak's OAuth authorization server functionality
- Mastering Keycloak's Identity Brokering functionality
- SAML 2 syntax and semantics
- Implement Keycloak metrics

Intended audience

This course is aimed at network managers, architects, design managers, system engineers and developers who need to integrate Keycloak or Red Hat Single Sign-On (RH-SSO).

Prerequisites

Basic knowledge of web architectures and Linux.

Course schedule

PARTICIPANTS

This course is aimed at network managers, architects, design managers, system engineers and developers who need to integrate Keycloak or Red Hat Single Sign-On (RH-SSO).

PREREQUISITES

Basic knowledge of web architectures and Linux.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant’s academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they’ve developed.

1 Installation

- The services provided by Keycloak.
- Standard protocols and the evolution of standard technologies.
- OAuth 2.0 authorization server.
- Identity provider: web SSO in IdP (identity provider) Initiated SSO or OP OpenID Connect.
- Identity Brokering.
- Clients, LDAP and the importance of digital signatures in Keycloak.

Hands-on work

Install, create LDAP directory instance, Keycloak/Quarkus instance. Synchronize LDAP users with Keycloak. Customize the Keycloak signature key (SAML and OIDC).

2 Standard protocols

- OAuth 2.0: syntax and concepts, Access Token Opaque or JWT, Refresh Token, scopes.
- OpenID Connect: syntax and concepts (ID Token, Authorization Code Flow/PKCE, Implicit Flow, Device Code Flow).
- Developments: CIBA, FAPI, OAuth 2.1.

Hands-on work

Configure Keycloak and a Password Flow OIDC application (shell script) as Code Flow OIDC (mod_auth_openidc Apache module), Implicit Flow OIDC (JavaScript app) and Device Flow (shell script).

3 SAML V2

- SAML V2 basic concepts.
- XML assertions.
- The identity provider (IdP).
- The service provider (SP).
- Bindings.
- IdPinitiated or SP initiated.
- Web SSO Profile and ECP Profile.

Hands-on work

Set up Keycloak's IdP SAML V2 (SAML V2 tracer in browser, install and configure SP mod_auth_mellon Apache, SP client4 in web SSO Profile, test IdP Initiated operation).

4 Cluster mode (HA)

- Keycloak architecture.
- Keycloak: from Wildfly and Quarkus, its database and Infinispan shared cache.

Hands-on work

Installation of 2 Keycloak servers in cluster mode (HA).

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

5 Keycloak administration

- Administration interfaces.
- Administration using the kcadm.sh command, via the Administration API.
- Delegation of administration.
- Authentication flow management.
- Back Channel Logout OIDC.
- Single Logout SAML V2.

Hands-on work
Administer Keycloak (export Realm MIRAMAR from H2 instance, import into cluster, test administration delegation, test authentication).

6 Authentication delegation (IDP)

- The identity broker concept.
- Keycloak's Identity Brokering services.
- Identity Brokering Keycloak/Keycloak (OIDC).
- Identity Brokering SAML Keycloak/Azure AD.
- Identity Brokering SAML Keycloak/Auth0.
- Link Identity Brokering module mod_auth_oidc and Keycloak.

Hands-on work
Implementation of SAML 2.0 authentication using Azure Active Directory (Azure AD), Keycloak / Auth0 and OpenID Connect Keycloak / Keycloak.

7 Audit and Monitoring

- Audit user events.
- Audit administration events.
- Setting up metrics
- Architecture and cohabitation Keycloak, Prometheus and Graphana.

Hands-on work
Implementation of Keycloak metrics. Supervision of user and administration events.

Dates and locations

REMOTE CLASS
2026 : 7 Apr., 16 June, 29 Sep., 15 Dec.