Keycloak, mise en œuvre

Cours Pratique de 4 jours - 28h
Réf : LDC - Prix 2024 : 2 790€ HT

Ce cours pratique présente Keycloak, la solution open source de gestion des identités et des accès (IAM) associés à l'implémentation des standards SAML 2. Cette formation vous permettra d'installer, configurer et superviser Keycloak de façon efficace dans un contexte d'entreprise.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Créer une instance de Keycloak

Maîtriser la fonctionnalité Serveur d'autorisation OAuth de Keycloak

Maîtriser la fonctionnalité Identity Brokering de Keycloak

Connaitre la syntaxe et sémantique de SAML 2

Mettre en œuvre des metrics Keycloak

LE PROGRAMME

dernière mise à jour : 06/2023

1) Installation

- Les services fournis par Keycloak.
- Les protocoles standards et l'évolution des technologies standards.
- Serveur d'autorisation OAuth 2.0.
- Fournisseur d'identité : web SSO en IdP (identity provider) Initiated SSO ou OP OpenID Connect.
- Courtage d'identité (Identity Brokering).
- Clients, LDAP et importance de la signature numérique dans Keycloak.

Travaux pratiques : Installer, créer une instance d'un annuaire LDAP, une instance de Keycloak/Quarkus. Synchroniser les utilisateurs LDAP avec Keycloak. Personnaliser la clef de signature Keycloak (SAML et OIDC).

2) Les protocoles standards

- OAuth 2.0 : la syntaxe et les concepts, Access Token Opaque ou JWT, Refresh Token, les scopes.
- OpenID Connect : syntaxe et concepts (ID Token, Authorization Code Flow/PKCE, Implicit Flow, Device Code Flow).
- Les évolutions : CIBA, FAPI, OAuth 2.1.

Travaux pratiques : Configurer Keycloak et une application Password Flow OIDC (script shell) en Code Flow OIDC (module Apache mod_auth_openidc), en Implicit Flow OIDC (app JavaScript) et en Device Flow (script shell).

3) SAML V2

- Les concepts de base SAML V2.
- Les assertions XML.
- L'identity provider (IdP).
- Le service provider (SP).
- Les bindings.
- IdPinitiated ou SP initiated.

PARTICIPANTS

Ce cours s'adresse aux responsables réseaux, architectes, responsables études, ingénieurs système et développeurs qui ont à intégrer le produit Keycloak ou le produit Red Hat Single Sign-On (RH-SSO).

PRÉREQUIS

Connaissances de base des architectures techniques web et de Linux.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Web SSO Profile et ECP Profile.
Travaux pratiques : Paramétrer IdP SAML V2 de Keycloak (traceur SAML V2 dans le navigateur, installer et configurer le SP mod_auth_mellon Apache, le SP client4 en web SSO Profile, tester le fonctionnement IdP Initiated).

4) Le mode Cluster (HA)
- Architecture de Keycloak.
- Keycloak : de Wildfly et Quarkus, sa base de données et le cache partagé Infinispan.
Travaux pratiques : Installation de 2 serveurs Keycloak en mode Cluster (HA).

5) Administration de Keycloak
- Interfaces d'administration.
- Administration via la commande kcadm.sh, via l'API d'administration.
- Délégation d'administration.
- Gestion des flux d'authentifications.
- Back Channel Logout OIDC.
- Single Logout SAML V2.
Travaux pratiques : Administrer Keycloak (exporter le Realm MIRAMAR de l'instance H2, importer dans le cluster, tester la délégation d'administration, tester l'authentification).

6) Délégation d'authentification (IDP)
- La notion de courtier d'identité (identity broker).
- Les services attendus de l'Identity Brokering de Keycloak.
- Identity Brokering Keycloak/Keycloak (OIDC).
- Identity Brokering SAML Keycloak/Azure AD.
- Identity Brokering SAML Keycloak/Auth0.
- Lien Identity Brokering module mod_auth_oidc et Keycloak.
Travaux pratiques : Mise en œuvre de l'authentification SAML 2.0 par Azure Active Directory (Azure AD), Keycloak / Auth0 et OpenID Connect Keycloak / Keycloak.

7) Audit et Monitoring
- Audit des événements utilisateurs.
- Audit des événements d'administration.
- Mise en place de metrics
- Architecture et cohabitation Keycloak, Prometheus et Graphana.
Travaux pratiques : Mise en place des metrics Keycloak. Supervision des événements utilisateurs et d'administration.

LES DATES

CLASSE À DISTANCE	PARIS
2024 : 11 juin, 17 sept., 03 déc.	2024 : 10 sept., 26 nov.