Gestion centralisée de la sécurité avec KeyCloak

Description

Keycloak est une solution open source de gestion des identités et des accès (IAM). Il implémente en standard les protocoles (OpenID Connect, OAuth 2.0, et SAML).
Les cas d'usage sont :

- Single-Sign On et délégation d'authentification (IdP)
- La fédération des utilisateurs
- Les mots de passe à usage unique (OTP)
- Gestion centralisée des autorisations aux services de l'entreprise

Cette formation, après avoir effectué un rappel sur les protocoles standard et la technologie JWT, détaille une à une les fonctionnalités de KeyCloak ainsi que leur mise en place. En s'appuyant sur des exemples concrets et des cas réels d'utilisation, la formation apporte toutes les connaissances nécessaires pour utiliser et exploiter Keycloak de façon efficace et résoudre les problématiques les plus souvent rencontrées.

Objectifs

- Avoir une vision complète des fonctionnalités et des cas d'usage de *Keycloak*
- Savoir mettre en place le SSO, plus précisément avec OpenID/Connect
- Savoir configurer les politiques d'accès à toutes les applications de l'entreprise (web, natif, API Rest)
- Être capable de mettre en production la solution

Public

Architectes, développeurs, exploitant de système

Pré-requis

- Avoir des connaissances de REST/HTTP
- Connaissance en architecture logicielle
- Avoir des connaissances minimum de Linux et des lignes de commandes

Travaux pratiques

De nombreux travaux pratiques (plus de 50%) sont proposés aux participants tout au long de la formation. Les solutions des ateliers seront fournies sous forme de dépôt Git, elles utilisent des applications web implémentées soit avec *Node.js* soit avec *Java/Spring*

Durée : 3 jours

Contenu de la formation

Introduction

- Aspects de la sécurité géré par *KeyCloak*, les différents acteurs de Keycloak
- Les protocoles supportés : SAML/OpenIDConnect, oAuth2, JWT
- Distribution et installation, les répertoires importants
- Console d'administration et concepts *Keycloak* : royaumes, clients, utilisateurs, rôles, groupes, scopes, consentement

Atelier *: Installation de la distribution all-in-one, sécurisation d'une première application*

Rappels sur les jetons

- JOSE et JWT
- Jeton d'accès, de rafraîchissement
- Offline_token
- Clé privé/public (rsa-generated)

Atelier *: Outils d'inspection et de validation des jetons*

Authentification et sécurisation des applications

- Adaptateurs et plateformes supportées, Comparaison OpenID et SAML2.0
- Flow d'authentification avec *OpenID*
- Le token ID, personnalisation du user profile, association de rôles
- Configuration du UserInfo endpoint
- Gestion du logout
- Politique dees mots de passe, Authentification forte avec *One Time Password*,

Atelier *: LogIn/Logout via OpenID, configuration d'une authentification forte*

Autorisation des accès avec oAuth2

- Retours sur le protocole *oAuth2* et les différents types de consentement
- Flow d'obtention du token avec l'*authorization code*
- Limitation des accès selon les audiences, les rôles, les scopes
- Validation du jeton

Atelier *: Protection des ressources d'une application web*

Sécurisation des différents types d'application

- Application web server-side
- Application web SPA avec API dédiée
- Applications mobiles et natives
- Sécurisation des micro-services

Atelier *: Protection des ressources d'une architecture micro-services*

Stratégies d’autorisation

- RBAC
- GBAC
- Scopes oAuth2
- ABAC

Atelier *: Utilisation d’ABAC pour les ACLs de l’architecture micro-services*

Keycloak pour la production

- Rappels Wildfly
- Typologie des endpoint : front-end, back-end et admin
- Mise en place de TLS
- Configuration de la base de données
- Intégration avec des annuaires externes
- Mise en cluster et Reverse proxy
- Test de l’architecture

Atelier *: Mise en place d’un cluster accédé via TLS*