KEYCLOAK & RED HAT SSO : Maîtrisez l'Authentification Centralisée et la Sécurité des Accès

Lien : https://innov-systems.com/formation/keycloak-red-hat-sso-maitrisez-lauthentification-centralisee-et-la-securite-des-acces

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**WLUM01**	**Red Hat Linux**

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les concepts fondamentaux de l'Identity and Access Management (IAM) et du Single Sign-On
- Maîtriser les protocoles d'authentification et d'autorisation OAuth 2.0, OpenID Connect et SAML 2.0
- Installer et configurer Keycloak en environnement de développement et production
- Créer et administrer des Realms, clients et utilisateurs dans Keycloak
- Configurer les flux d'authentification standards et personnalisés
- Mettre en place l'authentification multifacteur (MFA) avec OTP et WebAuthn
- Personnaliser l'interface utilisateur de Keycloak selon charte graphique entreprise
- Intégrer Keycloak avec annuaires d'entreprise LDAP et Microsoft Active Directory
- Configurer l'Identity Brokering avec des fournisseurs d'identité externes
- Sécuriser des applications Java (Spring Boot, ..) avec les adaptateurs Keycloak
- Protéger des applications JavaScript SPA avec keycloak-js et le flux PKCE
- Sécuriser des APIs REST avec validation de tokens JWT et gestion des scopes
- Concevoir une architecture Keycloak haute disponibilité en cluster
- Déployer Keycloak sur Kubernetes et OpenShift en respectant les bonnes pratiques
- Configurer une base de données de production avec réplication pour Keycloak
- Mettre en place le monitoring de Keycloak avec Prometheus et Grafana
- Configurer les logs d'audit et assurer la traçabilité des événements de sécurité
- Appliquer les bonnes pratiques de sécurité OWASP dans la configuration
- Diagnostiquer et résoudre les problèmes d'authentification et d'autorisation
- Concevoir une stratégie IAM alignée sur les principes Zero Trust

POUR QUI ?

- Architectes solutions et architectes sécurité concevant des systèmes d'authentification centralisée
- Développeurs Java (Spring Boot, Quarkus, Jakarta EE) devant sécuriser leurs applications
- Développeurs front-end (Angular, React, Vue.js) intégrant l'authentification SSO
- Administrateurs systèmes et réseaux responsables de l'infrastructure d'authentification
- Ingénieurs DevOps et DevSecOps déployant des solutions IAM en environnement conteneurisé
- Responsables sécurité des systèmes d'information (RSSI) supervisant les politiques d'accès
- Ingénieurs cloud déployant des applications sécurisées sur AWS, Azure ou GCP
- Chefs de projet techniques pilotant des projets de transformation digitale avec SSO
- Administrateurs d'annuaires (LDAP, Active Directory) intégrant des solutions de fédération
- Intégrateurs de solutions logicielles devant connecter plusieurs applications avec SSO

Programme détaillé

1 / FONDAMENTAUX DE L'IDENTITY AND ACCESS MANAGEMENT (IAM)

- Concepts clés de l'IAM : authentification, autorisation, fédération d'identités et Single Sign-On (SSO)
- Présentation des protocoles standards : OAuth 2.0 (RFC 6749), OpenID Connect (OIDC) et SAML 2.0
- Introduction à l'architecture Zero Trust et positionnement de Keycloak/Red Hat SSO dans l'écosystème IAM

2 / INSTALLATION ET CONFIGURATION DE KEYCLOAK

- Installation de Keycloak en mode standalone et en mode cluster (différentes distributions)
- Configuration initiale : console d'administration, paramètres système et bases de données supportées
- Déploiement avec Docker et premiers pas avec les conteneurs Keycloak officiels

3 / GESTION DES REALMS, CLIENTS ET UTILISATEURS

- Création et configuration des Realms : isolation des environnements et paramètres de sécurité
- Enregistrement et configuration des clients (applications) : types de clients, flows d'authentification et scopes
- Gestion des utilisateurs : création, attributs, groupes, rôles et permissions

4 / AUTHENTIFICATION ET FLUX DE CONNEXION

- Configuration des flux d'authentification : login, registration, reset password et authentification multifacteur (MFA)
- Mise en place de l'authentification à deux facteurs (OTP, WebAuthn, FIDO2)
- Personnalisation des thèmes et des pages de login selon la charte graphique de l'entreprise

5 / FÉDÉRATION D'IDENTITÉS ET IDENTITY BROKERING

- Intégration avec les annuaires d'entreprise : LDAP et Microsoft Active Directory

- Configuration de l'Identity Brokering : connexion avec fournisseurs externes (Google, Facebook, Azure AD, SAML IdP)
- Synchronisation des utilisateurs et mappage des attributs entre sources d'identité

6 / SÉCURISATION DES APPLICATIONS ET DES APIS

- Protection des applications Java (Spring Boot, Quarkus) avec les adaptateurs Keycloak
- Sécurisation des applications JavaScript (SPA) avec la bibliothèque keycloak-js et PKCE
- Protection des APIs REST : validation des tokens JWT, scopes et permissions fine-grained (UMA 2.0)

7 / HAUTE DISPONIBILITÉ ET DÉPLOIEMENT EN PRODUCTION

- Architecture haute disponibilité : clustering Keycloak avec Infinispan et répartition de charge
- Déploiement sur Kubernetes et OpenShift : Helm charts, opérateurs et bonnes pratiques
- Configuration des bases de données en production : PostgreSQL, MySQL/MariaDB avec réplication

8 / MONITORING, AUDIT ET CONFORMITÉ SÉCURITÉ

- Configuration des logs d'audit et traçabilité des événements de sécurité
- Intégration avec les outils de monitoring : Prometheus, Grafana et ELK Stack
- Conformité aux standards de sécurité : OWASP, RGPD et bonnes pratiques Red Hat

9 / CAS PRATIQUES ET LABS INTÉGRÉS

- Lab 1 : Mise en place complète d'un SSO pour un écosystème de 3 applications (Java, Angular, API REST)
- Lab 2 : Intégration de Keycloak avec Active Directory et configuration du MFA pour les utilisateurs
- Lab 3 : Déploiement d'un cluster Keycloak haute disponibilité sur Kubernetes avec monitoring

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

10 au 14 Août 2026	Présentiel -
12 au 16 Oct. 2026	Présentiel -
07 au 11 Déc. 2026	Présentiel -

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com