New

Keycloak, mise en oeuvre d’une gestion centralisée des accès utilisateurs

Centraliser l’authentification et piloter les identités

Présentiel ou en classe à distance

4 jours (28 h)

Prix inter : 3.050,00 € HT
Forfait intra : 8.890,00 € HT

Réf.: SR214

La formation **Keycloak - Mise en oeuvre et exploitation en environnement d’entreprise** propose une approche complète pour concevoir, déployer et administrer une **plateforme IAM** (Identity and Access Management) moderne basée sur **Keycloak**. Elle couvre les fondamentaux de la gestion des identités et des accès, les standards incontournables ainsi que l’intégration de Keycloak au sein d’architectures web et cloud d’entreprise. Les participants acquièrent une compréhension claire du positionnement de Keycloak comme **Identity Provider central**, capable d’assurer l’authentification.
Au-delà du déploiement, la formation met l’accent sur l’**exploitation avancée** de la solution : fédération LDAP, identity brokering avec des IdP externes (Azure AD, Auth0), mise en place du **MFA**, sécurisation de l’administration, gestion des rôles et des claims, haute disponibilité en mode cluster, sauvegarde, supervision et monitoring avec Prometheus et Grafana. Les nombreux travaux pratiques permettent de concevoir une architecture cible, de déployer un environnement complet et de le préparer à la production.

A qui s'adresse cette formation ?

Pour qui

- Développeurs, administrateurs, architectes IAM

Prérequis

- Des connaissances de base en architectures web, en environnement Linux et des notions IAM
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - IAM et positionnement de Keycloak

- Enjeux de la gestion des identités en entreprise
- Rôles IAM : IdP, SP, clients, ressources
- Différences authentification / autorisation
- Présentation des standards :
- OAuth 2.0
- OpenID Connect
- SAML v2
- Place de Keycloak dans un SI moderne

Atelier

Analyse d’un SI existant et identification des points d’intégration IAM

Choix des protocoles adaptés selon les cas d’usage

2 - Architecture Keycloak pour l’entreprise

- Composants internes de Keycloak
- Notion de realm et stratégies multi-realm
- Architecture mono-instance vs cluster
- Bases de données supportées
- Séparation dev / test / prod
  Atelier

  Schéma d’architecture cible Keycloak pour un contexte entreprise

3 - Déploiement et configuration initiale

- Déploiement avec Docker
- Configuration de la base de données
- Paramétrage initial du serveur
- Accès et sécurisation de la console d’administration
- Gestion des secrets et variables d’environnement
  Atelier

  Déploiement complet d’une instance Keycloak

  Validation du fonctionnement et persistance des données

4 - Gestion des utilisateurs, groupes et rôles

- Création et organisation des utilisateurs
- Groupes, rôles realm et rôles client
- Mapping des rôles
- Attributs utilisateurs et claims
  Atelier

  Modélisation d’une organisation réelle

  Tests d’authentification et analyse des tokens JWT

5 - Sécurisation des applications et SSO

- Types de clients (confidential, public, bearer-only)
- Flux OAuth / OIDC
- Mise en oeuvre du Single Sign-On
- Gestion des sessions
- Déconnexion globale (Single Logout)
  Atelier

  Connexion de plusieurs applications à un même realm

  Validation du SSO et du logout global

6 - Fédération des identités avec LDAP

- Principe de la fédération d’identités
- Intégration d’un annuaire LDAP
- Synchronisation des utilisateurs
- Mapping des attributs LDAP
- Cas des comptes hybrides (local + LDAP)
  Atelier

  Connexion à un LDAP

  Import et synchronisation des comptes

  Tests d’authentification LDAP

7 - Identity Brokering et IdP externes

- Principe de l’Identity Brokering
- Chaînage d’authentification
- Intégration : Keycloak ↔ Keycloak
- Azure AD
- Auth0

- Gestion des utilisateurs fédérés
  Atelier

  Mise en place d’un Identity Provider externe

  Tests d’authentification déléguée

8 - SAML v2 en pratique

- Concepts SAML (Assertions, SP, IdP)
- Différences SAML / OIDC
- Cas d’usage SAML en entreprise
- Configuration SAML dans Keycloak
  Atelier

  Configuration d’un client SAML

  Analyse des échanges SAML

9 - Politiques de sécurité et MFA

- Politiques de mot de passe
- OTP et MFA
- Flows d’authentification Keycloak
- Adaptation des flows selon les profils
  Atelier

  Création d’un flow personnalisé

  Activation du MFA pour des populations ciblées

10 - Sécurisation de l’administration

- Sécurisation des comptes admins
- Séparation des rôles d’administration
- Bonnes pratiques d’accès à la console Audit des actions d’administration
  Atelier

  Mise en conformité d’une console d’administration

11 - Keycloak en cluster

- Concepts de haute disponibilité
- Mode cluster Keycloak
- Gestion des sessions distribuées
- Points de vigilance (sticky sessions, DB, cache)
  Atelier

  Étude d’une architecture cluster

  Analyse des risques et contraintes

12 - Sauvegarde et reprise

- Sauvegarde des configurations
- Export / import de realms
- Stratégies de restauration
- Continuité de service
  Atelier

  Sauvegarde et restauration d’un environnement Keycloak

13 - Logs, audit et traçabilité

- Types de logs Keycloak
- Audit des événements d’authentification
- Analyse des incidents
- Conformité et traçabilité
  Atelier

  Analyse de journaux réels

Investigation d’un incident d’authentification

14 - Monitoring et métriques

- Exposition des métriques Keycloak
- Intégration Prometheus
- Tableaux de bord Grafana
- Indicateurs clés de santé IAM

Atelier

Mise en place d’un dashboard de supervision

15 - Mise en production et bonnes pratiques

- Checklist de mise en production
- Sécurisation finale
- Performance et montée en charge
- Erreurs courantes et anti-patterns

Atelier

Validation complète d’un environnement prêt pour la production

Les objectifs de la formation

- Déployer une instance Keycloak adaptée à un contexte d’entreprise
- Gérer les utilisateurs, rôles et groupes avec une modélisation fine des droits
- Sécuriser des applications via OAuth2, OIDC, SAML et le Single Sign-On
- Intégrer une fédération d’identités avec un annuaire LDAP ou un IdP externe
- Concevoir des flows d’authentification incluant MFA et règles de sécurité avancées
- Superviser, auditer et maintenir une architecture Keycloak en haute disponibilité

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- L'apprentissage par la pratique : les phases théoriques sont complétées d'ateliers favorisant un ancrage durable des acquis
- Une formation animée par des formateurs experts IAM et Keycloak

Dates et villes 2026 - Référence SR214

Dernières places disponibles Session garantie

A distance

du 2 mars au 5 mars	du 6 juil. au 9 juil.	du 26 oct. au 29 oct.
du 27 avr. au 30 avr.	du 24 août au 27 août	du 16 nov. au 19 nov.

Paris

du 2 mars au 5 mars	du 6 juil. au 9 juil.	du 26 oct. au 29 oct.
du 27 avr. au 30 avr.	du 24 août au 27 août	du 16 nov. au 19 nov.