+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 21/09/2023

S'inscrire

Formation Keycloak Avancé

2 jours (14 heures)

PRÉSENTATION

Sécurisez simplement vos applications avec l'outil open-source, Keycloak. Avec Keycloak, vous pourrez empêcher des accès non autorisés et ainsi vous protéger des cyberattaques.

Créé et mis à jour par Red Hat, l'outil supporte trois protocoles d'authentification : SAML, OAuth 2 et OpenID.

Keycloak possède de nombreuses fonctionnalités comme une prise en charge complète du SSO (Single Sign-On et Single Sign-Out), un gestionnaire d'identité et d'accès des utilisateurs permettant de créer une base de données d'utilisateurs avec des rôles et des groupes personnalisés ou encore l'utilisation du LDAP et d'Active Directory.

Notre formation Keycloak avancée vous enseignera l'utilisation avancée de Keycloak avec la présentation du keycloak logger, l'user storage federation, le scope client ou encore la gestion des autorisations

Notre formation Keycloak avancée présentera la dernière version de l'outil, Keycloak 22.0.

OBJECTIFS

- Maîtriser le cycle de vie des jetons d'accès et de rafraîchissement
- Configurer et mettre en œuvre différentes stratégies d'autorisation
- Assurer la sécurité des applications sensibles avec Keycloak en se conformant à la norme FAPI
- Utiliser les API REST d'administration de Keycloak pour la gestion avancée des autorisations

PUBLIC VISÉ

- Développeurs
- Architectes techniques

- Chefs de projet
- Administrateurs

Pré-requis

- Dans l'idéal, avoir suivi notre formation Keycloak
- Connaissances en protocole de sécurité
- Avoir déjà utilisé Keycloak
- Bonnes connaissances en Windows et Linux/UNIX
- Bonnes compétences en TCP/IP
- Bonne maîtrise en HTTP
- Connaissance en architecture logicielle

Pré-requis logiciels

- Avoir Java installé
- Docker Desktop ou Podman installés sur vos PCs

PROGRAMME DE NOTRE FORMATION KEYCLOAK AVANCÉ

Utilisation avancée des jetons OAuth

- Comprendre le cycle de vie
  - Des jetons d'accès
  - Des jetons de rafraîchissement
- Configurer Keycloak pour générer/valider des jeton de type offline_access
- Mettre en œuvre l'exchange_token

Mise en œuvre des autorisations fines

- Rappel des protocoles
  - OAuth 2.0
  - OpenID Connect
- Comprendre les concepts de rôles, de permissions et de politiques dans Keycloak
- Configurer et mettre en œuvre différentes stratégies d'autorisation avec Keycloak
- Déléguer la gestion des autorisations à l'utilisateur avec la norme UMA 2.0

Sécuriser les applications sensibles avec Keycloak

- Introduction à FAPI (Financial-grade API) et aux exigences de sécurité
- Mise en œuvre des exigences de la norme FAPI dans Keycloak
- Établir des tests de sécurité automatisés pour les mécanismes d'autorisation

Mise en œuvre des API REST Admin de Keycloak

- Présentation des API REST de Keycloak
- Test des requêtes les plus utiliser via les API REST

Personnalisation de Keycloak

- Personnaliser la page de connexion et les templates des emails
- Configurer des flux d'authentification personnalisée
- Étendre les fonctionnalités de Keycloak avec les SPI (Service Provider Interfaces)

Module complémentaire (+1 jour)

Le scope client

- Présentation des scopes et des claims
- Le protocole
- Lier le scope client avec le client
- Les permissions
- Utiliser les scopes et les claims
- Authentification avec le numéro de téléphone
- Keycloak generator pour évaluer le scope

Gestion des autorisations avancée

- Comprendre en détail l'UMA avec Keycloak
- Utiliser les permissions
- Approbation ou révocation
- Accéder au UMA grâce au REST API
- Services d'autorisation
- Évaluer et tester les policies
- Renforcement des policies

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.