

Mis à jour le 29/11/2023

S'inscrire

Formation Auth0 : Maîtrisez l'authentification et l'autorisation

2 jours (14 heures)

PRÉSENTATION

Notre formation Auth0 vous dotera des compétences essentielles pour maîtriser la gestion de l'identité et de l'accès, en utilisant la puissante [plateforme Auth0](#).

Au cours de cette formation, vous développerez une expertise approfondie dans le domaine de l'authentification en explorant en détail les fonctionnalités et les concepts clés d'Auth0, et en apprenant à les mettre en pratique dans vos projets.

Vous découvrirez comment configurer et personnaliser Auth0 pour répondre aux besoins spécifiques de votre application, tout en garantissant la sécurité et la convivialité pour vos utilisateurs.

Cette formation vous permettra de comprendre comment Auth0 simplifie l'authentification et l'autorisation, et comment l'utiliser pour créer des solutions sécurisées et conviviales.

Comme dans toutes nos formations, nous vous fournirons les [dernières ressources](#) et les meilleures pratiques d'Auth0.

OBJECTIFS

- Comprendre Auth0 et son importance dans l'authentification centralisée
- Maîtriser la configuration d'un compte et d'une application Auth0
- Mettre en œuvre le protocole Auth0 depuis une application frontale
- Développer les compétences pour intégrer Auth0 via API
- Comprendre et appliquer l'authentification multifacteur (MFA)

PUBLIC VISÉ

- Développeurs
- Administrateurs système
- Responsables et experts en cybersécurité

Pré-requis

- Une solide compréhension des concepts de développement logiciel
- Une connaissance de base des concepts liés à l'authentification et à la sécurité serait un avantage supplémentaire

PROGRAMME DE NOTRE FORMATION AUTH0

PRÉSENTATION GÉNÉRALE

- Qu'est-ce qu'Auth0 ?
- Pourquoi utiliser Auth0 ?
- Avantages de l'authentification centralisée
- Historique et évolution d'Auth0
- Vue d'ensemble de l'industrie de l'authentification
- Rôles et responsabilités dans la gestion d'Auth0

CONFIGURATION

- Création d'un compte Auth0
- Création d'une application Auth0
- Configuration des paramètres de base
- Gestion des environnements de développement et de production
- Pratiques recommandées en matière de configuration
- Personnalisation du domaine d'authentification

MISE EN PLACE DU PROTOCOLE AUTH0 DEPUIS UNE APPLICATION FRONT

- Intégration avec des applications frontales
- Comprendre et utiliser un JWT (JSON Web Token)
- Mise en œuvre de l'authentification à deux facteurs
- Intégration de l'authentification sociale
- Configuration des politiques d'autorisation
- Gestion des autorisations basées sur les rôles
- Sécurisation des tokens d'authentification
- Compréhension des flux d'authentification

INTÉGRATION SUR API

- Intégration personnalisée via API
- Utilisation des webhooks pour les événements
- Personnalisation des courriels de notification
- Intégration avec des services d'annuaires externes
- Personnalisation des pages d'erreur

MFA

- Authentification multifacteur (MFA)
- Stratégies de gestion des mots de passe
- Utiliser le JWT pour les droits d'accès
- Gestion des rôles et droits via AuthO

API LOCK

- Intégration rapide avec Module Lock
- Migration vers Auth0 depuis un environnement existant
- Personnalisation de l'interface utilisateur d'Auth0

PRÉSENTATION DES DIFFÉRENTS PROVIDERS

- AWS
- GCP
- Azure

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.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

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.