

Mis à jour le 18/08/2026

S'inscrire

Formation Certification WSO2 Identity Server Practitioner

2 jours (14 heures)

Présentation

WSO2 Identity Server est une solution IAM open source conçue pour sécuriser les parcours d'authentification, de fédération et de contrôle d'accès. Avec cette certification officielle, vous validez votre capacité à comprendre l'architecture, les usages et les mécanismes clés de la plateforme.

Notre formation Certification WSO2 Identity Server Practitioner vous prépare de manière ciblée à l'examen WSO2 Certified Identity Server Practitioner, avec une approche orientée validation des acquis et mise en situation.

Vous apprendrez à maîtriser les fondamentaux de WSO2 Identity Server, à exploiter les principaux flux d'authentification, à gérer les utilisateurs, les applications et les fournisseurs d'identité, ainsi qu'à comprendre les grands principes de la fédération et de la délégation d'accès.

La formation vous guide également sur les notions attendues à l'examen, comme les standards d'identité, la configuration de la plateforme, les extensions, les customisations et les bonnes pratiques de déploiement dans un contexte de production.

À l'issue de ce parcours, vous serez mieux préparé pour réussir la certification, expliquer les cas d'usage métier de la solution et intervenir avec méthode sur un projet IAM basé sur WSO2 Identity Server.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre le positionnement fonctionnel de WSO2 Identity Server dans un écosystème IAM.
- Identifier les concepts essentiels de l'authentification, de la fédération et du contrôle d'accès.
- Configurer les principaux éléments de la plateforme pour couvrir des cas d'usage courants.
- Préparer efficacement l'examen WSO2 Certified Identity Server Practitioner avec une logique de révision ciblée.
- Analyser un besoin métier et relier les exigences de sécurité aux capacités du produit.

Public visé

- Développeur IAM
- Architecte sécurité
- Consultant identité numérique
- Administrateur système
- Chef de projet technique

Pré-requis

- Connaissances de base en IAM et en gestion des identités.
- Notions générales sur les protocoles SAML, OAuth 2.0 et OpenID Connect.
- Expérience préalable en administration ou en paramétrage d'une solution de sécurité ou d'authentification.
- Compréhension des enjeux d'intégration applicative et de contrôle d'accès.
- Capacité à lire une documentation technique en anglais.

Pré-requis techniques

- Un ordinateur récent avec navigateur web à jour et droits d'installation locaux.
- Une connexion Internet stable en Wi-Fi ou Ethernet pour les labs et les ressources en ligne.
- Un environnement de travail permettant d'exécuter un client de test, par exemple Postman ou un navigateur moderne.
- Un micro et un casque si la session est suivie à distance.
- Un accès utilisateur à la plateforme de formation ou aux environnements fournis pendant le cours.

Programme de notre formation WSO2 Identity Server Practitioner

[Jour 1 - Matin]

Fondamentaux de la plateforme

- Positionnement de WSO2 Identity Server dans une architecture IAM.
- Rappels sur les cas d'usage couverts par la solution, SSO, fédération, gestion des accès.

- Présentation des composants fonctionnels attendus à l'examen WSO2 Certified Identity Server Practitioner.
- Lecture d'une architecture type, rôles, flux et dépendances principales.
- Distinction entre besoins métier, exigences de sécurité et capacités produit.
- Atelier pratique : cartographier un cas d'usage d'entreprise et relier chaque besoin à une fonction de WSO2 Identity Server.

[Jour 1 - Après-midi]

Gestion des utilisateurs et authentification

- Modèle utilisateur, comptes, attributs et notions de base sur les annuaires.
- Principes de gestion des identités et des credentials dans la plateforme.
- Parcours d'authentification, facteurs, enchaînements et règles de décision.
- Vue d'ensemble des standards SAML, OAuth 2.0 et OpenID Connect.
- Premiers réflexes de configuration pour sécuriser un accès applicatif.
- Atelier pratique : configurer un scénario d'authentification simple et vérifier le comportement d'un flux de connexion.

[Jour 2 - Matin]

Fédération et contrôle d'accès

- Comprendre la fédération d'identité et le rôle des fournisseurs d'identité.
- Configurer les échanges entre application, IdP et service provider.
- Découvrir les principes de délégation d'accès et de gestion des autorisations.
- Analyser les mécanismes de politiques, règles et décisions d'accès.
- Identifier les points de vigilance liés à la sécurité et à la cohérence des flux.
- Atelier pratique : mettre en place une fédération de test et valider le parcours d'authentification de bout en bout.

[Jour 2 - Après-midi]

Révision examen et mise en situation

- Revue structurée des notions les plus susceptibles d'être évaluées à l'examen.
- Questions types sur l'architecture, les usages et les mécanismes de configuration.
- Bonnes pratiques pour lire rapidement un énoncé et éliminer les distracteurs.
- Méthode de révision ciblée sur les zones de connaissance prioritaires.
- Conseils pour aborder l'examen WSO2 Certified Identity Server Practitioner avec méthode.
- Atelier pratique : réaliser un mini-examen blanc corrigé et justifier chaque réponse à partir des concepts vus en formation.

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.