Administrateur des identités et des accès Microsoft (SC-300T00)

Durée: 4 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

Ce cours s'adresse aux administrateurs des identités et des accès qui prévoient de passer l'examen de certification associé, ou qui effectuent des tâches d'administration des identités et des accès dans leur travail quotidien. Ce cours serait également utile à un administrateur ou à un ingénieur qui souhaite se spécialiser dans la fourniture de solutions d'identité et de systèmes de gestion des accès pour les solutions basées sur Azure, jouant ainsi un rôle essentiel dans la protection d'une organisation.

Objectifs de la formation

À la fin de ce cours, les participants seront en mesure de:

- Concevoir, mettre en œuvre et exploiter des solutions de gestion de l’identité et des accès (IAM) à l’aide de Microsoft Entra ID
- Configurer et gérer l’authentification et l’autorisation sécurisées pour les applications d’entreprise
- Offrir des expériences utilisateur fluides et des capacités d’autogestion dans l’organisation
- Mettre en œuvre des stratégies d’accès adaptatif et de gouvernance de l’identité pour protéger les ressources organisationnelles
- Surveiller, dépanner et produire des rapports sur les environnements d’identité et d’accès afin d’assurer fiabilité et conformité
- Collaborer efficacement avec des rôles interfonctionnels pour soutenir des initiatives stratégiques en matière d’identité

Description sommaire

Le cours Administrateur des identités et des accès Microsoft explore comment concevoir, mettre en œuvre et exploiter les systèmes de gestion de l’identité et des accès d’une organisation en utilisant Microsoft Entra ID. Apprenez à gérer des tâches telles que l’authentification sécurisée et l’autorisation

Copyright © 2026 AFI par Edgenda inc.

d’accès aux applications d’entreprise. Vous apprendrez également à offrir des expériences fluides et des capacités d’autogestion pour tous les utilisateurs. Enfin, découvrez comment créer un accès adaptatif et une gouvernance de vos solutions de gestion de l’identité et des accès, afin d’assurer le dépannage, la surveillance et la production de rapports sur votre environnement.

L’administrateur de l’identité et de l’accès peut être une seule personne ou un membre d’une équipe plus large. Découvrez comment ce rôle collabore avec plusieurs autres rôles dans l’organisation pour mener des projets stratégiques liés à l’identité. L’objectif final est de vous fournir les connaissances nécessaires pour moderniser les solutions d’identité, mettre en œuvre des solutions d’identité hybrides et instaurer une gouvernance de l’identité.

Contenu du plan de cours

Parcours d’apprentissage 1 — Explorer l’identité dans Microsoft Entra ID

- Module 1 — Explorer l’identité dans Microsoft Entra ID

Parcours d’apprentissage 2 — Mettre en œuvre une solution de gestion de l’identité avec Microsoft Entra ID

- Module 1 — Mettre en œuvre la configuration initiale de Microsoft Entra ID
- Module 2 — Créer, configurer et gérer les identités
- Module 3 — Mettre en œuvre et gérer les identités externes
- Module 4 — Mettre en œuvre et gérer l’identité hybride

Parcours d’apprentissage 3 — Mettre en œuvre une solution d’authentification et de gestion des accès

- Module 1 — Sécuriser les utilisateurs Microsoft Entra avec l’authentification multifacteur
- Module 2 — Gérer l’authentification des utilisateurs

Copyright © 2026 AFI par Edgenda inc.

- Module 3 — Planifier, mettre en œuvre et administrer l’accès conditionnel
- Module 4 — Gérer Microsoft Entra Identity Protection
- Module 5 — Mettre en œuvre la gestion des accès pour les ressources Azure
- Module 6 — Déployer et configurer Microsoft Entra Global Secure Access

Parcours d’apprentissage 4 — Mettre en œuvre la gestion des accès pour les applications

- Module 1 — Planifier et concevoir l’intégration des applications d’entreprise pour le SSO
- Module 2 — Mettre en œuvre et surveiller l’intégration des applications d’entreprise pour le SSO
- Module 3 — Mettre en œuvre l’enregistrement des applications
- Module 4 — Enregistrer des applications à l’aide de Microsoft Entra ID

Parcours d’apprentissage 5 — Planifier et mettre en œuvre une stratégie de gouvernance de l’identité

- Module 1 — Planifier et mettre en œuvre la gestion des droits (entitlement management)
- Module 2 — Planifier, mettre en œuvre et gérer les revues d’accès
- Module 3 — Planifier et mettre en œuvre l’accès privilégié
- Module 4 — Surveiller et maintenir Microsoft Entra ID

Approche et méthode pédagogique

Copyright © 2026 AFI par Edgenda inc.

Approche pratique et structurée combinant théorie ciblée et ateliers guidés. Les participants administrent progressivement les identités et les accès Microsoft au moyen d'exercices inspirés de scénarios professionnels, favorisant une application immédiate des apprentissages.

Ils apprennent à gérer les identités, sécuriser l'accès, mettre en œuvre l'authentification et la gouvernance avec Microsoft Entra ID.

Animée par un formateur certifié Microsoft (MCT), la formation met l'accent sur l'interactivité et le développement de compétences techniques directement transférables pour protéger efficacement les ressources et les utilisateurs en contexte professionnel..

Prérequis

Les participants doivent posséder les connaissances et l'expérience suivantes avant de suivre ce cours :

- Comprendre les meilleures pratiques de sécurité et les exigences de l'industrie (défense en profondeur, accès privilégié minimal, contrôle d'accès basé sur les rôles, responsabilité partagée, modèle Zero Trust)
- Être familiers avec les fournisseurs d'identité tels que Microsoft Entra ID, Microsoft Entra Domain Services ou d'autres fournisseurs d'authentification
- Avoir une certaine expérience du déploiement de charges de travail Azure
- Avoir de l'expérience avec les systèmes d'exploitation Windows et/ou Linux et une expérience minimale en scripts
- Avoir de l'expérience avec PowerShell et la CLI

Recommandations

Prérequis facultatifs :

- Connaissance générale de Microsoft Entra ID
- Compréhension pratique de l'intégration des applications d'entreprise et des concepts SSO
- Connaissances de base en gouvernance de l'identité (gestion des droits, revues d'accès)

Copyright © 2026 AFI par Edgenda inc.

- Sensibilisation aux principes Zero Trust et aux stratégies d’accès adaptatif
- Exposition préalable aux concepts d’authentification multifacteur (MFA)

Certifications

Microsoft Certifié : Administrateur d'Identité et d'Accès Associé

Notes légales

© AFI Expertise inc.

Copyright © 2026 AFI par Edgenda inc.