

# Configurer et gérer les droits avec Microsoft Entra ID (SC-5008)

Durée: 1 jour

Public cible: Professionnel TI

## À qui s'adresse cette formation ?

Cette formation s'adresse aux personnes qui souhaitent mettre en œuvre une solution complète de gestion des habilitations fondée sur les principes du modèle Zero Trust.

Les participants doivent posséder une expérience avec Azure ainsi qu'une expérience dans la création d'identités et l'attribution d'accès à des ressources pour ces identités.

## Objectifs de la formation

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

- Configurer et gérer la gestion des habilitations Microsoft Entra afin d'optimiser l'accès des utilisateurs tout en soutenant les principes de sécurité Zero Trust.
- Mettre en œuvre des révisions d'accès et des contrôles d'accès privilégié afin de maintenir le principe du moindre privilège et de renforcer la sécurité organisationnelle.
- Surveiller et traiter les événements de sécurité liés à l'identité et aux accès en appliquant les meilleures pratiques pour améliorer la conformité et la posture de sécurité.

## Description sommaire

Dans le paysage numérique actuel, la gestion des accès et des habilitations est essentielle pour protéger les renseignements sensibles et assurer la conformité. Cette formation intensive d'une journée offre une étude approfondie de la gestion des habilitations Microsoft Entra, des révisions d'accès, de l'accès privilégié et de la surveillance.

Les participants apprendront à optimiser la gestion des accès grâce à la gestion des habilitations, à effectuer des révisions d'accès approfondies afin de maintenir le principe du moindre privilège, à gérer les accès privilégiés à haut risque et à mettre en œuvre des stratégies de surveillance robustes permettant de détecter et de répondre rapidement aux événements de sécurité.

À la fin de cette formation, les participants disposeront des meilleures pratiques et de recommandations concrètes pour renforcer la posture de sécurité de leur organisation.

## **Contenu du plan de cours**

### **Parcours d'apprentissage 1 : Configurer et gouverner les habilitations avec Microsoft Entra ID**

- Module 1 : Planifier et mettre en œuvre la gestion des habilitations
- Module 2 : Planifier, mettre en œuvre et gérer les révisions d'accès
- Module 3 : Surveiller et maintenir Microsoft Entra ID
- Module 4 : Planifier et mettre en œuvre l'accès privilégié

## **Approche et méthode pédagogique**

Approche pratique et structurée combinant théorie ciblée et ateliers guidés. Les participants découvrent progressivement comment concevoir et gérer des solutions analytiques avec Power BI grâce à des exercices pratiques inspirés de situations d'affaires réelles, favorisant une mise en application immédiate des apprentissages.

Ils apprennent à préparer et à modéliser les données, à créer des visualisations percutantes, à développer des rapports et tableaux de bord interactifs, ainsi qu'à appliquer des techniques d'analyse pour soutenir une prise de décision basée sur les données.

Animée par un Microsoft Certified Trainer (MCT), cette formation met l'accent sur l'interactivité et le développement de compétences pratiques transférables permettant d'utiliser efficacement Power BI dans un environnement professionnel.

## **Prérequis**

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

-

Comprendre les meilleures pratiques de sécurité ainsi que les exigences de l'industrie en matière de sécurité, notamment la défense en profondeur, le principe du moindre privilège, le contrôle d'accès basé sur les rôles (RBAC), le modèle de responsabilité partagée et le modèle Zero Trust.

- Être familier avec les fournisseurs d'identité tels que Microsoft Entra ID, Microsoft Entra Domain Services ou d'autres fournisseurs d'authentification.
- Avoir de l'expérience avec les systèmes d'exploitation Windows ou Linux ainsi qu'une connaissance de base des langages de script. Cette formation aborde notamment l'utilisation de PowerShell et de l'interface de ligne de commande (CLI).

## **Recommandations**

- Connaître les concepts de sécurité et de gestion des accès.
- Être à l'aise avec les environnements Microsoft 365 / Azure.
- Comprendre les notions de gouvernance des accès (cycle de vie, permissions).
- Avoir une expérience en administration ou en sécurité IT (atout).

## **Notes légales**

© AFI Expertise inc.